

AVG Anti-Virus 2011

Benutzerhandbuch

Dokumentversion 2011.21 (16.5.2011)



Inhalt











1. Einleitung

Dieses Benutzerhandbuch bietet eine umfassende Dokumentation zu **AVG Anti-Virus 2011**.

Herzlichen Glückwunsch zum Kauf von AVG Anti-Virus 2011!

AVG Anti-Virus 2011 zählt zu einer Reihe von preisgekrönten AVG-Produkten, die vollständige Sicherheit für Ihren PC bieten, damit Sie in Ruhe arbeiten können. Wie alle AVG-Produkte wurde **AVG Anti-Virus 2011** von Grund auf vollkommen neu gestaltet, um den anerkannten Schutz von AVG noch benutzerfreundlicher und effizienter bereitzustellen. Ihr neues **AVG Anti-Virus 2011**-Produkt verfügt über eine optimierte Benutzeroberfläche sowie aggressivere und schnellere Scans. Die Anzahl der automatisierten Sicherheitsfunktionen wurde zu Ihrer Unterstützung erhöht und neue ‚intelligente' Benutzeroptionen hinzugefügt, damit Sie unsere Sicherheitsfunktionen besser an Ihre Bedürfnisse anpassen können. Einfache Verwendung und hohe Sicherheit schließen einander nicht aus!

AVG wurde entwickelt, um Ihre Computer- und Netzwerkaktivitäten zu schützen. Genießen Sie den vollständigen Rundumschutz von AVG.

Alle AVG-Produkte bieten folgende Vorteile:

- Schutz für den individuellen Umgang mit Ihrem Computer und dem Internet: Banking, Shopping, Surfen und Suchen, Chatten, Mailen, Dateien herunterladen oder Aktivitäten in sozialen Netzwerken – AVG liefert das richtige Produkt für Ihren individuellen Bedarf
- Sorgenfreier Schutz, dem mehr als 110 Millionen Menschen auf der ganzen Welt vertrauen und der ständig von einem globalen Netzwerk erfahrener Researcher weiterentwickelt wird
- Schutz mit Experten-Support rund um die Uhr



2. Installationsvoraussetzungen für AVG

2.1. Unterstützte Betriebssysteme

AVG Anti-Virus 2011 wurde für den Schutz von Workstations mit den folgenden Betriebssystemen entwickelt:

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 und x64, alle Editionen)
- Windows 7 (x86 und x64, alle Editionen)

(sowie ggf. höhere Service Packs für bestimmte Betriebssysteme)

***Hinweis**: Die Komponente Identitätsschutz wird unter Windows XP x64 nicht unterstützt. Bei diesem Betriebssystem können Sie AVG Anti-Virus 2011 installieren, jedoch ohne die Komponente „Identitätsschutz".*

2.2. Minimale und empfohlene Hardware-Anforderungen

Minimale Hardware-Anforderungen für **AVG Anti-Virus 2011**:

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM-Speicher
- 750 MB an freiem Festplattenplatz (für die Installation)

Empfohlene Hardware-Anforderungen für **AVG Anti-Virus 2011**:

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM-Speicher
- 1400 MB an freiem Festplattenplatz (für die Installation)



3. Optionen für die Installation von AVG

AVG kann entweder mithilfe der Installationsdatei installiert werden, die sich auf Ihrer Installations-CD befindet, oder Sie können die neueste Installationsdatei von der Website von AVG (http://www.avg.com/de/) herunterladen.

Vor der Installation von AVG sollten Sie auf jeden Fall prüfen, ob auf der Website von AVG (http://www.avg.com/de/) eine neue Installationsdatei verfügbar ist. Auf diese Weise können Sie sicher sein, dass Sie die neueste verfügbare Version von AVG Anti-Virus 2011 installieren.

Während des Installationsvorgangs werden Sie nach Ihrer Lizenz-/Vertriebsnummer gefragt. Halten Sie diese bereit, bevor Sie mit der Installation beginnen. Die Vertriebsnummer befindet sich auf der Verpackung der CD. Wenn Sie AVG online erworben haben, wurde Ihnen die Lizenznummer per eMail zugeschickt.



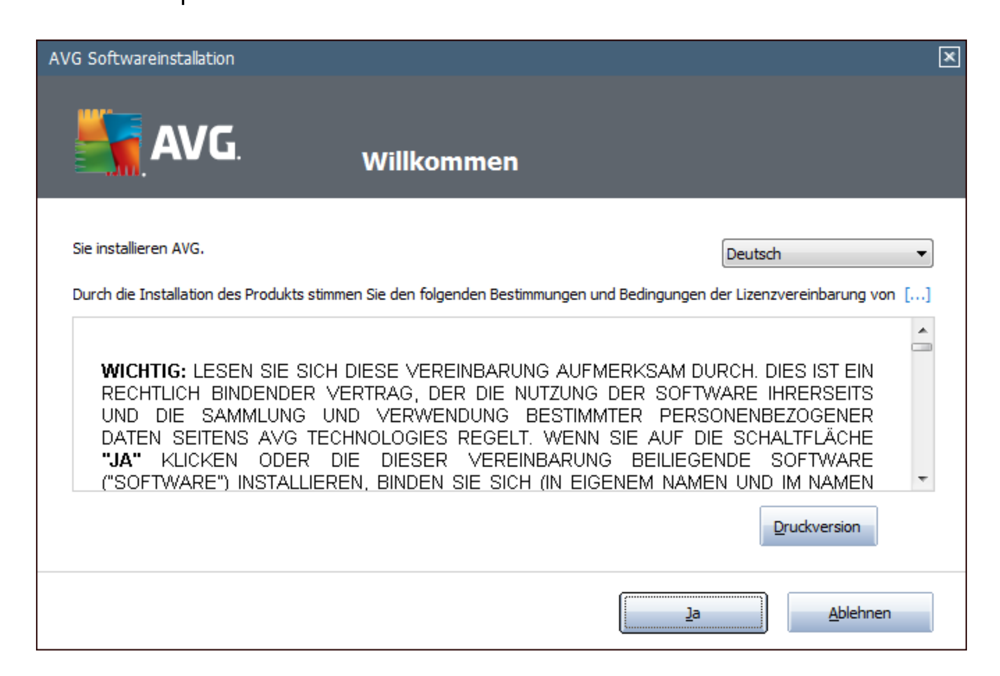
4. Installationsvorgang bei AVG

Für die Installation von **AVG Anti-Virus 2011** auf Ihrem Computer benötigen Sie die aktuellste Installationsdatei. Sie können die Installationsdatei auf der CD verwenden, die Bestandteil Ihrer Edition ist. Diese Datei ist jedoch möglicherweise nicht mehr aktuell. Es wird daher empfohlen, die aktuellste Installationsdatei online herunterzuladen. Sie können die Datei von der Website von AVG (http://www.avg.com/de/) im Bereich ***Support Center / Downloads*** herunterladen.

Der Installationsvorgang besteht aus einer Abfolge von Dialogen, die jeweils eine kurze Beschreibung der erforderlichen Schritte enthalten. Im Folgenden werden die einzelnen Dialoge erläutert:

4.1. Willkommen

Zu Beginn des Installationsvorgangs wird das Dialogfenster ***Willkommen*** angezeigt. Hier können Sie die Sprache für die Installation und die Standardsprache für die Benutzeroberfläche von AVG auswählen. Im oberen Bereich des Dialogs befindet sich ein Dropdown-Menü mit den zur Auswahl stehenden Sprachen:



Achtung: *Hier wählen Sie nur die Sprache für den Installationsvorgang aus. Die ausgewählte Sprache wird als Standardsprache für die Benutzeroberfläche von AVG installiert. Daneben wird Englisch immer automatisch installiert. Wenn Sie weitere Sprachen für die Benutzeroberfläche installieren möchten, geben Sie die gewünschten Sprachen in einen der folgenden Setup-Dialoge* ***Benutzerdefinierte Optionen*** *an.*

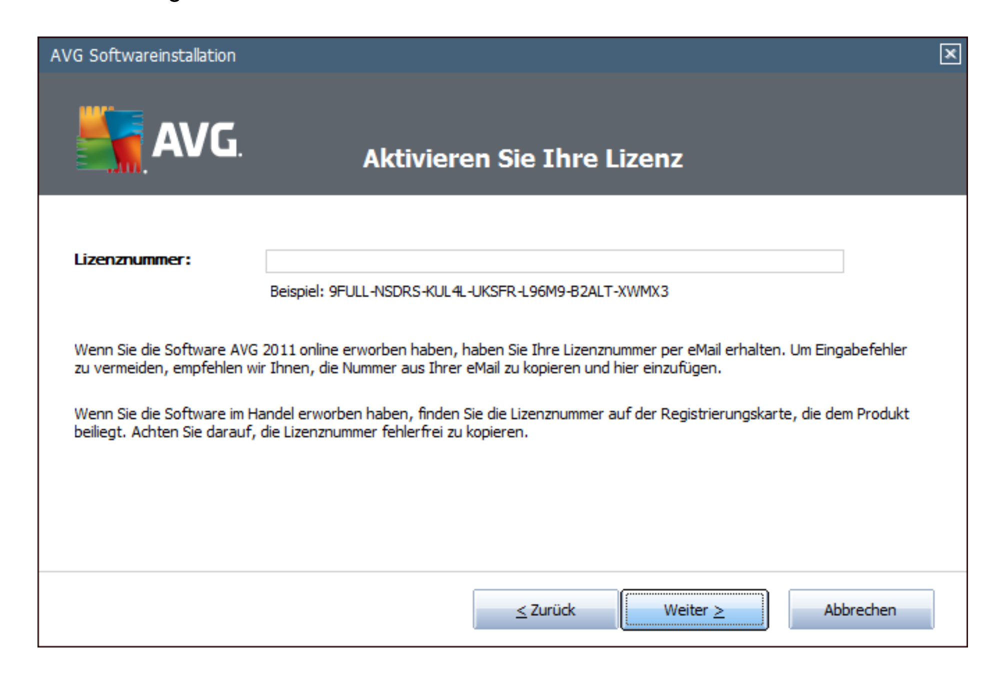
Dieser Dialog enthält auch den vollständigen Text der Lizenzvereinbarung von AVG. Lesen Sie das Dokument sorgfältig durch. Klicken Sie auf ***Akzeptieren***, um zu bestätigen, dass Sie die Vereinbarung gelesen, verstanden und akzeptiert haben. Falls Sie der Lizenzvereinbarung nicht zustimmen, klicken Sie auf ***Ablehnen***, und der Installationsvorgang wird abgebrochen.



4.2. AVG-Lizenz aktivieren

Im Dialog ***AVG-Lizenz aktivieren*** werden Sie dazu aufgefordert, Ihre Lizenznummer in das dafür vorgesehene Feld einzugeben.

Die Vertriebsnummer finden Sie auf der CD-Verpackung Ihres **AVG Anti-Virus 2011**-Pakets. Die Lizenznummer ist in der Bestätigungs-eMail enthalten, die Sie nach dem Online-Kauf von **AVG Anti-Virus 2011** erhalten haben. Sie müssen die Nummer exakt wie dargestellt eingeben. Wenn die Lizenznummer in digitaler Form verfügbar ist (*in der eMail*), empfehlen wir Ihnen, diese zu kopieren und einzufügen.



Klicken Sie auf ***Weiter***, um mit der Installation fortzufahren.



4.3. Wählen Sie die Installationsart aus



Der Dialog ***Wählen Sie die Installationsart aus*** bietet zwei Installationsoptionen: ***Schnellinstallation*** und ***Benutzerdefinierte Installation***.

Den meisten Benutzern wird empfohlen, die standardmäßige ***Schnellinstallation*** beizubehalten, mit der AVG vollständig automatisch mit den vom Programmhersteller vordefinierten Einstellungen installiert wird. Diese Konfiguration bietet die höchste Sicherheit, verbunden mit einer optimalen Ressourcennutzung. Wenn die Konfiguration zukünftig geändert werden muss, können Sie diese Änderungen immer direkt in der Anwendung AVG vornehmen. Wenn Sie die Option ***Schnellinstallation*** ausgewählt haben, klicken Sie auf ***Weiter***, um mit dem Dialog ***AVG Security Toolbar installieren*** fortzufahren.

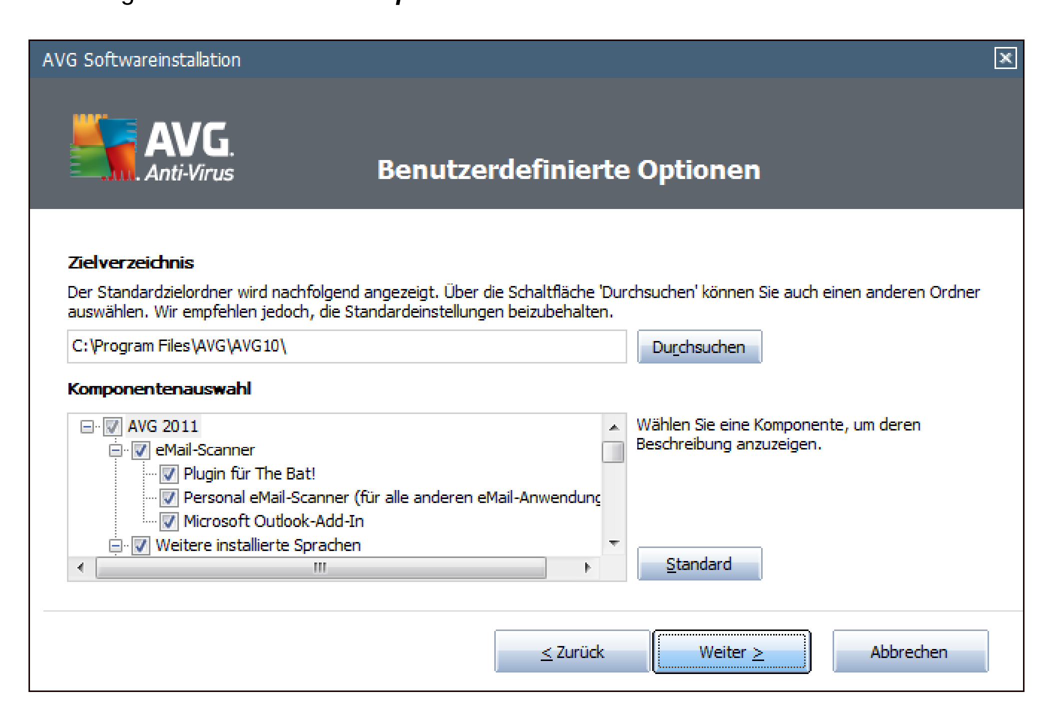
Die ***Benutzerdefinierte Installation*** sollte nur von erfahrenen Benutzern verwendet werden, die einen wichtigen Grund haben, AVG nicht mit den Standardeinstellungen zu installieren, beispielsweise um bestimmte Systemanforderungen zu erfüllen. Wenn Sie diese Option ausgewählt haben, klicken Sie auf ***Weiter***, um mit dem Dialog ***Benutzerdefinierte Optionen*** fortzufahren.

Im rechten Bereich des Dialogs finden Sie das Kontrollkästchen zum ***AVG-Gadget*** (*unterstützt unter Windows Vista und Windows 7*). Aktivieren Sie dieses Kontrollkästchen, wenn Sie das Gadget installieren möchten. Das ***AVG-Gadget*** wird daraufhin über die Windows-Sidebar verfügbar sein und bietet Ihnen Zugriff auf die wichtigsten Features von **AVG Anti-Virus 2011** wie Scans und Updates.



4.4. Benutzerdefinierte Optionen

Im Dialog ***Benutzerdefinierte Optionen*** können Sie zwei Parameter für die Installation festlegen:



Zielverzeichnis

Im Dialogabschnitt ***Zielverzeichnis*** können Sie den Speicherort angeben, an dem **AVG Anti-Virus 2011** installiert werden soll. Standardmäßig wird AVG im Ordner C:/Programme installiert. Wenn Sie einen anderen Speicherort angeben möchten, klicken Sie auf ***Durchsuchen***, um die Verzeichnisstruktur anzuzeigen, und wählen Sie den gewünschten Ordner aus.

Komponentenauswahl

Im Abschnitt ***Komponentenauswahl*** wird eine Übersicht über alle Komponenten von **AVG Anti-Virus 2011** angezeigt, die installiert werden können. Wenn die Standardeinstellungen nicht Ihren Anforderungen entsprechen, können Sie einzelne Komponenten entfernen oder hinzufügen.

Sie können jedoch nur Komponenten auswählen, die in Ihrer AVG Edition enthalten sind!

Markieren Sie einen Eintrag in der Liste ***Komponentenauswahl***, um eine kurze Beschreibung der entsprechenden Komponente auf der rechten Seite dieses Bereichs anzuzeigen. Weitere Informationen zu den Funktionen der einzelnen Komponenten finden Sie im Kapitel ***Komponentenübersicht*** in dieser Dokumentation. Klicken Sie auf die Schaltfläche ***Standard***, um die werkseitigen Standardeinstellungen wiederherzustellen.

Klicken Sie zum Fortfahren auf ***Weiter***.



4.5. AVG Security Toolbar installieren



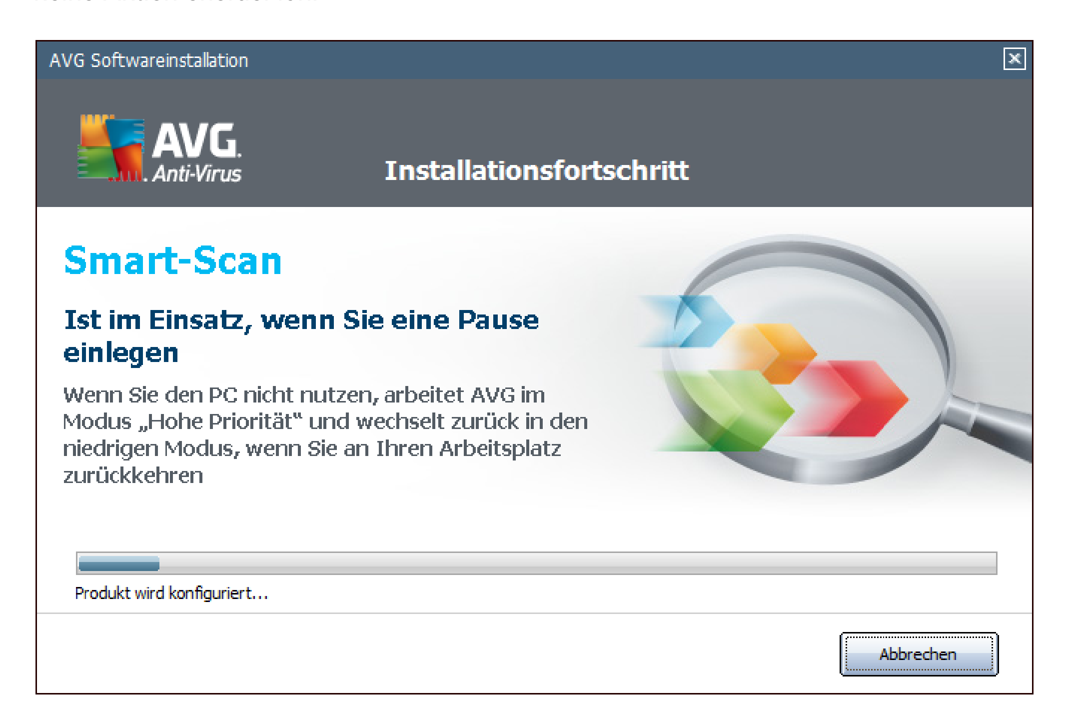
Entscheiden Sie im Dialog ***AVG Security Toolbar installieren***, ob Sie die ***AVG Security Toolbar*** installieren möchten. Wenn Sie die Standardeinstellungen nicht ändern, wird die Komponente automatisch in Ihrem Internetbrowser installiert (*derzeit werden die Browser Microsoft Internet Explorer 6.0 oder höher, Mozilla Firefox 3.0 oder höher unterstützt*), so dass Sie beim Surfen im Internet umfassend geschützt sind.

Sie können zudem entscheiden, ob Sie *AVG Secure Search (powered by Google)* als Ihren Standard-Suchanbieter festlegen möchten. Behalten Sie in diesem Fall die Aktivierung des entsprechenden Kontrollkästchens bei.



4.6. Installationsfortschritt

Im Dialog ***Installationsfortschritt*** wird der Fortschritt des Installationsvorgangs angezeigt. Hier ist keine Aktion erforderlich:



Nach Abschluss des Installationsvorgangs werden Sie zum nächsten Dialog weitergeleitet.

4.7. Die Installation wurde erfolgreich abgeschlossen





Der Dialog ***Die Installation wurde erfolgreich abgeschlossen*** bestätigt, dass **AVG Anti-Virus 2011** vollständig installiert und konfiguriert wurde.

Geben Sie in diesem Dialog Ihre Kontaktinformationen ein, so dass Sie über die neuesten Produktinformationen benachrichtigt werden können. Unter dem Formular zur Registrierung stehen die folgenden zwei Optionen zur Verfügung:

- ***Ja, halten Sie mich über Neuigkeiten zur Sicherheit und über spezielle Angebote zu AVG 2011 per eMail auf dem Laufenden*** – Aktivieren Sie diese Option, wenn Sie über Neuigkeiten in Bezug auf Internetsicherheit informiert werden möchten und Informationen zu Sonderangeboten zu AVG-Produkten, Verbesserungen und Upgrades usw. erhalten möchten.

- ***Ich stimme der Teilnahme an AVG 2011-Websicherheit und am Programm zur Produktverbesserung zu*** – Aktivieren Sie dieses Kontrollkästchen, wenn Sie am Programm zur Produktverbesserung teilnehmen möchten (*Weitere Informationen finden Sie in KapitelErweiterte Einstellungen von AVG/Programm zur Produktverbesserung*), wobei anonyme Informationen zu erkannten Bedrohungen gesammelt werden, um die allgemeine Sicherheit im Internet zu verbessern.

Starten Sie zum Abschließen des Installationsvorgang Ihren Computer neu: Wählen Sie entweder ***Jetzt neu starten*** oder ***Später neu starten*** aus.

> ***Hinweis:***
> *·Wenn·Sie·eine·geschäftliche·Lizenz·für·AVG·verwenden·und·bereits·vorher·ausgewählt·habe n,·die·Komponente·„Remote-Verwaltung“·zu·installieren·(Benutzerdefinierte Optionen) wird in der folgenden Benutzeroberfläche der Dialog „Die Installation wurde erfolgreich abgeschlossen“ angezeigt:*
>
> *Geben Sie AVG DataCenter-Parameter an – Geben Sie die Verbindungszeichenkette zum AVG DataCenter in der Form „Server:Port“ an. Wenn diese Informationen momentan nicht verfügbar sind, lassen Sie das Feld leer, und nehmen Sie die Konfiguration später im Dialog* ***Erweiterte Einstellungen/Remote-Verwaltung*** *vor. Genaue Informationen zur Remote-Verwaltung von AVG erhalten Sie im Benutzerhandbuch der AVG Business Edition, das Sie von der AVG-Website (http://www.avg.com/de/) herunterladen können.*



5. Nach der Installation

5.1. Produktregistrierung

Nach Abschluss der Installation von **AVG Anti-Virus 2011** registrieren Sie bitte Ihr Produkt, indem Sie auf der Website von AVG (http://www.avg.com/de/) die Seite ***Registrierung*** aufrufen (*folgen Sie den Anweisungen auf dieser Seite*). Nach der Registrierung erhalten Sie vollen Zugriff auf Ihr AVG-Benutzerkonto, den AVG Update-Newsletter und andere exklusive Dienste für registrierte Benutzer.

5.2. Zugriff auf die Benutzeroberfläche

Die***Benutzeroberfläche von AVG*** kann auf mehrere Arten geöffnet werden:

- durch Doppelklicken auf das ***AVG-Symbol im Infobereich***
- durch Doppelklicken auf das AVG-Symbol auf dem Desktop
- durch Doppelklicken auf die Statuszeile im unteren Bereich des ***AVG-Gadget*** (*falls installiert; wird unter Windows Vista und Windows 7 unterstützt*)
- über das Menü ***Start/Alle Programme/AVG 2011/Benutzeroberfläche von AVG***
- von der ***AVG Security Toolbar*** über die Option ***AVG starten***

5.3. Gesamten Computer scannen

Es besteht das potentielle Risiko, dass vor der Installation von **AVG Anti-Virus 2011** bereits ein Virus auf Ihren Computer übertragen wurde. Aus diesem Grund sollten Sie die Option ***Gesamten Computer scannen*** ausführen, um sicherzustellen, dass Ihr Computer nicht infiziert ist.

Eine Anleitung, wie Sie die Option ***Gesamten Computer scannen*** ausführen, finden Sie im Kapitel ***AVG-Scans***.

5.4. Eicar-Test

Zur Überprüfung, ob **AVG Anti-Virus 2011** korrekt installiert wurde, können Sie den EICAR-Test durchführen.

Der EICAR-Test ist eine standardmäßige und absolut sichere Methode, um die Funktion von Virenschutzsystemen zu überprüfen. Es kann ohne Sicherheitsrisiko weitergegeben werden, da es sich dabei nicht um ein wirkliches Virus handelt und es auch keine Fragmente viralen Codes enthält. Die meisten Produkte reagieren jedoch, als würde es sich tatsächlich um ein Virus handeln (*es wird in der Regel mit einem offensichtlichen Namen wie „EICAR-AV-Test“ gemeldet*). Sie können das EICAR-Virus von der EICAR-Website unter www.eicar.com herunterladen und finden dort auch alle wichtigen Informationen zum EICAR-Test.

Laden Sie die Datei ***eicar.com*** herunter und speichern Sie sie auf Ihrer lokalen Festplatte. Unmittelbar nachdem Sie den Download der Testdatei bestätigt haben, reagiert ***Online Shield***



darauf mit einer Warnung. Diese Meldung zeigt an, dass AVG korrekt auf dem Computer installiert ist.



Von der Website http://www.eicar.com können Sie auch eine komprimierte Version des EICAR-, Virus' herunterladen (*im Format eicar_com.zip*). ***Online Shield*** gibt Ihnen die Möglichkeit, diese Datei herunterzuladen und auf Ihrer Festplatte zu speichern. Beim Entpacken der Datei wird der , Virus' jedoch vom ***Residenten Schutz*** erkannt. **Wenn AVG die EICAR-Testdatei nicht als Virus erkennt, sollten Sie die Programmkonfiguration überprüfen!**

5.5. Standardkonfiguration von AVG

Die Standardkonfiguration (*Konfiguration der Anwendung unmittelbar nach der Installation*) von**AVG Anti-Virus 2011** ist vom Händler so eingestellt, dass alle Komponenten und Funktionen eine optimale Leistung erzielen.

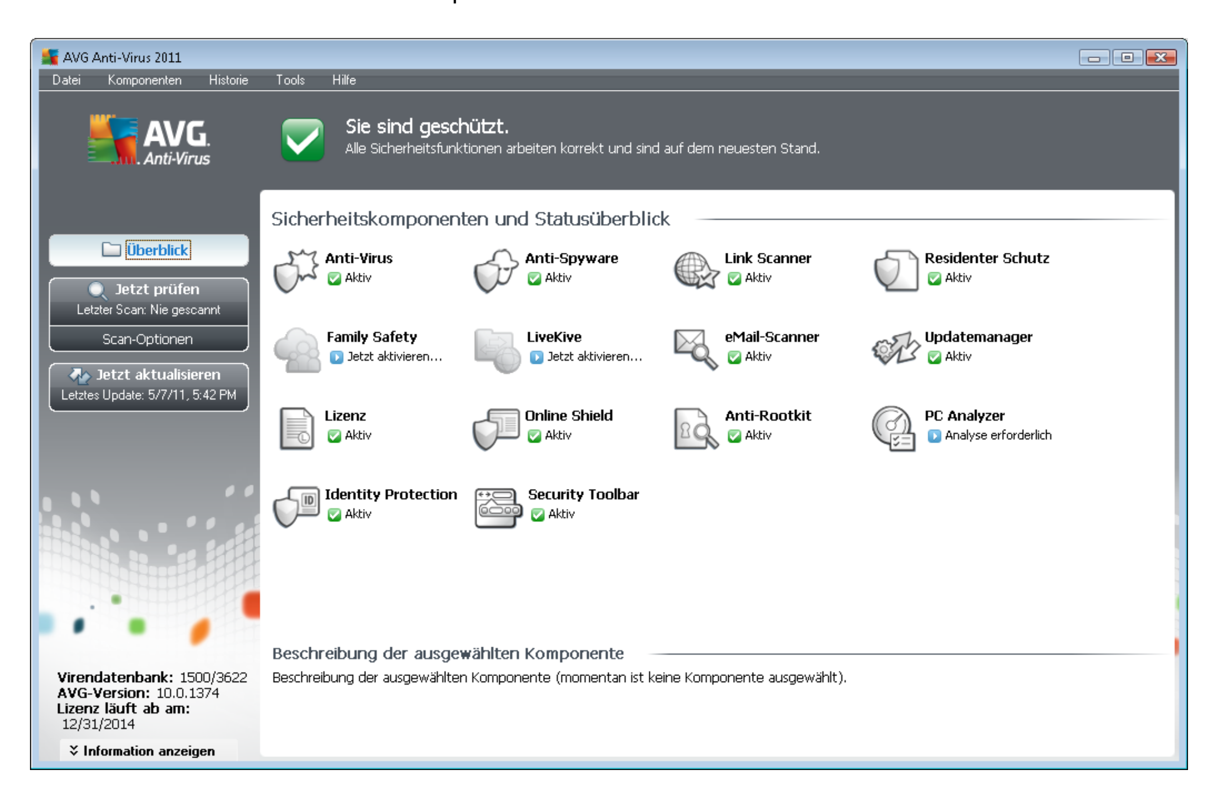
Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben! Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.

Geringfügige Änderungen an den Einstellungen der ***Komponenten von AVG*** können direkt über die Benutzeroberfläche der jeweiligen Komponente festgelegt werden. Wenn Sie die Konfiguration von AVG ändern und besser an Ihre Bedürfnisse anpassen möchten, wechseln Sie zu ***Erweiterte AVG-Einstellungen***, und wählen Sie im Systemmenü ***Tools/Erweiterte Einstellungen*** aus. Daraufhin wird der Dialog ***Erweiterte AVG-Einstellungen*** angezeigt, in dem Sie die Konfiguration von AVG ändern können.



6. Benutzeroberfläche von AVG

AVG Anti-Virus 2011 öffnet das Hauptfenster:



Das Hauptfenster ist in mehrere Bereiche gegliedert:

- ***Systemmenü*** *(Leiste an der Oberseite des Fensters)* dient zur Standardnavigation für den Zugriff auf alle Komponenten, Dienste und Funktionen von AVG - Details >>
- ***Informationen zum Sicherheitsstatus*** *(oberer Bereich des Fensters)* enthält Informationen zum aktuellen Status Ihres AVG-Programms - Details >>
- ***Quick Links*** *(linker Bereich des Fensters)* ermöglichen das schnelle Aufrufen der wichtigsten und am häufigsten verwendeten AVG-Aufgaben - Details >>
- ***Komponentenübersicht*** *(zentraler Bereich des Fensters)* zeigt eine Übersicht über alle installierten Komponenten von AVG - Details >>
- ***Statistik*** *(linker unterer Bereich des Fensters)* enthält alle statistischen Daten zur Programmnutzung - Details >>
- ***Infobereich-Symbol*** *(untere rechte Ecke des Bildschirms, im Infobereich)* zeigt den aktuellen Status von AVG - Details >>
- Δασ ***AVG-Gadget****(Windows-Sidebar, wird unter Windows Vista und Windows 7 unterstützt)* ermöglicht schnellen Zugriff auf AVG-Scans und -Updates – Details >>



6.1. Systemmenü

Das ***Systemmenü*** ist die Standardnavigation, die in allen Anwendungen von Windows verwendet wird. Es befindet sich horizontal im oberen Teil des Hauptfensters von **AVG Anti-Virus 2011**. Mit Hilfe des Systemmenüs können Sie auf bestimmte Komponenten, Funktionen und Dienste von AVG zugreifen.

Das Systemmenü ist in fünf Hauptbereiche eingeteilt:

6.1.1. Datei

- ***Beenden*** – Schließt die Benutzeroberfläche von **AVG Anti-Virus 2011**. Die AVG-Anwendung wird jedoch weiterhin im Hintergrund ausgeführt, damit Ihr Computer geschützt ist!

6.1.2. Komponenten

Der Menüpunkt ***Komponenten*** des Systemmenüs enthält Links zu allen installierten Komponenten von AVG, wobei jeweils der Standarddialog in der Benutzeroberfläche geöffnet wird:

- ***Systemüberblick*** – öffnet den Standarddialog der Benutzeroberfläche mit einer Übersicht über alle installierten Komponenten und deren Status
- ***Anti-Virus*** stellt sicher, dass Ihr Computer vor Viren geschützt wird – Details >>
- ***Anti-Spyware*** gewährleistet, dass Ihr Computer vor Spyware und Adware geschützt ist – Details >>
- ***Link Scanner*** überprüft die Suchergebnisse, die in Ihrem Internetbrowser angezeigt werden – Details >>
- ***eMail-Scanner*** überprüft alle eingehenden und ausgehenden eMails auf Viren – Details >>
- ***Family Safety*** unterstützt Sie beim Überwachen der Online-Aktivitäten Ihrer Kinder und schützt diese vor ungeeigneten Webinhalten – Details >>
- ***LiveKive*** bietet automatische Backups Ihrer Online-Daten – Details >>
- ***Residenter Schutz*** wird im Hintergrund ausgeführt und scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden – Details >>
- ***Updatemanager*** kontrolliert alle Aktualisierungen von AVG – Details >>
- ***Lizenz*** zeigt die Lizenznummer, den Lizenztyp und das Ablaufdatum an – Details >>
- ***Online Shield*** scannt alle Daten, die mit einem Webbrowser heruntergeladen werden – Details >>
- ***Anti-Rootkit*** erkennt Programme und Technologien, die darauf abzielen, Malware zu verbergen – Details >>



- ***PC Analyzer*** bietet Informationen zum Status Ihres Computers – Details >>

- ***Identitätsschutz*** – Eine Komponente für Anti-Malware, mit der Ihre persönlichen digitalen Daten vor Identitätsdiebstahl geschützt werden – Details >>

- ***Security Toolbar*** ermöglicht es Ihnen, ausgewählte Funktion von AVG direkt in Ihrem Internetbrowser zu verwenden – Details >>

- ***Remote-Verwaltung*** wird nur in AVG Business Editions angezeigt, wenn Sie beim Installationsvorgang angegeben haben, dass diese Komponente installiert werden soll

6.1.3. Historie

- ***Scan-Ergebnisse*** - Wechsel zur Testoberfläche von AVG, und zwar zum Dialog ***Übersicht über Scan-Ergebnisse***

- ***Residenter Schutz*** – Anzeigen eines Dialogs mit einer Übersicht über Bedrohungen, erkannt durch den ***Residenten Schutz***

- ***eMail-Scanner*** – Öffnet einen Dialog mit einer Übersicht über eMail-Anhänge, die von der Komponente ***eMail-Scanner*** als gefährlich erkannt wurden

- ***Funde des Online Shield*** – Öffnet einen Dialog mit einer Übersicht über Bedrohungen, die von ***Online Shield***

- ***Virenquarantäne*** - Anzeige der Oberfläche der Virenquarantäne (***Virenquarantäne***), in die AVG alle erkannten Infektionen verschiebt, die nicht automatisch geheilt werden können. Innerhalb dieser Quarantäne werden die infizierten Dateien isoliert, so das die Sicherheit Ihres Computers gewährleistet ist. Gleichzeitig werden die infizierten Dateien für eine mögliche Reparatur gespeichert

- ***Ereignisprotokoll*** – Anzeige der Ereignisprotokoll-Oberfläche mit einer Übersicht über alle protokollierten Aktionen von **AVG Anti-Virus 2011**

6.1.4. Tools

- ***Computer scannen*** – wechselt zur Scan-Oberfläche von AVG und startet einen Scan des gesamten Computers.

- ***Ausgewählten Ordner scannen*** – Wechselt zur Scan-Oberfläche von AVG , wo Sie in der Baumstruktur Ihres Computers entscheiden können, welche Dateien und Ordner gescannt werden sollen.

- ***Datei scannen*** – Dabei können Sie in der Baumstruktur Ihres Laufwerks eine einzelne Datei auswählen und einen On-Demand-Scan durchführen.

- ***Aktualisieren*** – startet automatisch den Aktualisierungsvorgang von **AVG Anti-Virus 2011**.

- ***Aus Verzeichnis aktualisieren*** – führt den Aktualisierungsvorgang von den Aktualisierungsdateien aus, die sich in einem dafür vorgesehenen Ordner auf Ihrem lokalen Laufwerk befinden. Die Verwendung dieser Option empfehlen wir Ihnen jedoch nur in Notfällen, z. B. wenn keine Verbindung zum Internet vorhanden ist (*beispielsweise wenn Ihr*



Computer infiziert ist und die Verbindung zum Internet verloren hat oder Ihr Computer mit einem Netzwerk verbunden ist, das keinen Zugang zum Internet hat). Wählen Sie im neu geöffneten Fenster den Ordner, in dem Sie die Aktualisierungsdatei zuvor gespeichert haben, und starten Sie den Aktualisierungsvorgang.

- ***Erweiterte Einstellungen*** – Öffnet den Dialog ***Erweiterte AVG-Einstellungen*** , in dem Sie die Konfiguration von **AVG Anti-Virus 2011** bearbeiten können. Im Allgemeinen empfehlen wir Ihnen, die Standardeinstellungen der Software beizubehalten, die vom Software-Hersteller festgelegt wurden.

6.1.5. Hilfe

- ***Inhalt*** – öffnet die Hilfedateien von AVG
- ***Onlinehilfe*** – Öffnet die Website von AVG (http://www.avg.com/de/) auf der Hauptseite des Kundendienstes
- ***Ihr AVG-Web*** – Öffnet die Startseite der Website von AVG (http://www.avg.com/de/)
- ***Virenenzyklopädie*** – öffnet die Online-***Virenenzyklopädie*** , aus der Sie genaue Informationen über das ermittelte Virus abrufen können
- ***Erneut aktivieren*** – Öffnet den Dialog ***AVG aktivieren*** mit den Daten, die Sie im Dialog ***AVG personalisieren*** des Installationsvorgangs eingegeben haben. In diesem Dialog können Sie Ihre Lizenznummer eingeben, um entweder die Vertriebsnummer (*die Nummer, mit der Sie AVG installiert haben*) oder die alte Lizenznummer (*zum Beispiel beim Upgrade auf ein neues AVG-Produkt*) zu ersetzen.
- ***Jetzt registrieren*** – Stellt eine Verbindung zur Registrierungsseite der Website von AVG (http://www.avg.com/de/) her. Bitte geben Sie Ihre Registrierungsdaten ein; nur Kunden, die ihr AVG-Produkt registrieren, erhalten kostenlosen technischen Support.

Hinweis*: Wenn Sie die Testversion von* **AVG Anti-Virus 2011** *verwenden, werden die letzten zwei Einträge als* ***Jetzt kaufen*** *und* ***Aktivieren*** *angezeigt und ermöglichen es Ihnen, die Vollversion des Programms zu erwerben. Wenn* **AVG Anti-Virus 2011** *mit einer Vertriebsnummer installiert ist, werden die Einträge als* ***Registrieren*** *und* ***Aktivieren*** *angezeigt. Weitere Informationen finden Sie im Abschnitt* *Lizenz* *dieser Dokumentation.*

- ***Info zu AVG*** – Öffnet den Dialog ***Information*** mit fünf Reitern, die Informationen über den Namen des Programms, das Programm selbst und die Version der Virendatenbank sowie Systeminformationen, die Lizenzvereinbarung und Kontaktdaten von ***AVG Technologies CZ*** enthalten.

6.2. Informationen zum Sicherheitsstatus

Der Bereich ***Informationen zum Sicherheitsstatus*** befindet sich im oberen Teil des Hauptfensters von AVG. In diesem Bereich finden Sie stets Informationen zum aktuellen Sicherheitsstatus von **AVG Anti-Virus 2011**. Bitte verschaffen Sie sich eine Übersicht über Symbole, die in diesem Bereich möglicherweise angezeigt werden und über ihre Bedeutung:



- Das grüne Symbol zeigt an, dass Ihr AVG vollständig funktioniert. Alle Sicherheitsfunktionen arbeiten korrekt und sind auf dem neuesten Stand.

- Das orangefarbene Symbol warnt Sie, wenn eine oder mehrere Komponenten falsch konfiguriert sind. Überprüfen Sie deren Eigenschaften/Einstellungen. Es besteht kein grundlegendes Problem in AVG, und Sie haben sich wahrscheinlich entschieden, einige Komponenten aus bestimmten Gründen zu deaktivieren. Sie sind immer noch durch AVG geschützt. Sie sollten jedoch die Einstellungen der problematischen Komponente überprüfen! Den Namen der Komponente finden Sie im Bereich ***Informationen zum Sicherheitsstatus***.

Dieses Symbol wird auch dann angezeigt, wenn Sie sich aus einem bestimmten Grund dazu entschieden haben, den Fehlerstatus einer Komponente zu ignorieren (*die Option „Komponentenstatus ignorieren" ist im Kontextmenü verfügbar, das Sie durch einen Klick mit der rechten Maustaste auf das Komponentensymbol in der Komponentenübersicht des Hauptfensters von AVG öffnen können*). Es kann vorkommen, dass Sie diese Option in bestimmten Situationen verwenden müssen, aber es wird dringend empfohlen, die Option „***Komponentenstatus ignorieren***" so bald wie möglich zu deaktivieren.

- Das rote Symbol zeigt an, dass sich AVG in einem kritischen Status befindet! Eine oder mehrere Komponenten werden nicht korrekt ausgeführt, und AVG kann Ihren Computer nicht schützen. Bitte beheben Sie unverzüglich das berichtete Problem. Wenn Sie den Fehler nicht selbst beheben können, wenden Sie sich an den Technischen Support von AVG.

Wenn AVG nicht für eine optimale Leistung konfiguriert ist, wird neben den Sicherheitsstatusinformationen eine neue Schaltfläche „Reparieren" angezeigt (alternativ auch „Alles reparieren", wenn das Problem mehrere Komponenten betrifft). Klicken Sie auf diese Schaltfläche, um einen automatischen Vorgang zur Programmüberprüfung und -konfiguration zu starten. Anhand dieser einfachen Methode können Sie AVG für eine optimale Leistung optimieren und maximale Sicherheit erzielen.

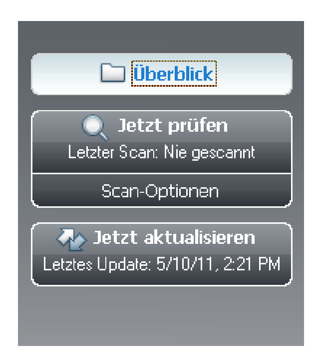
Es ist äußerst empfehlenswert, auf die Informationen zum Sicherheitsstatus zu achten und ein angezeigtes Problem unverzüglich zu lösen. Anderenfalls ist Ihr Computer gefährdet!

Hinweis: *Statusinformationen von AVG erhalten Sie auch jederzeit über das Symbol im Infobereich.*



6.3. Quick Links

***Mithilfe der Quick Links** (im linken Bereich der [Benutzeroberfläche von AVG](#))* können Sie sofort auf die wichtigsten und am häufigsten verwendeten Features von AVG zugreifen:



- ***Überblick*** – Mit diesem Link können Sie von jeder aktuell geöffneten Oberfläche von AVG zur Standardoberfläche wechseln, auf der Sie eine Übersicht über alle installierten Komponenten erhalten. Siehe Kapitel [***Komponentenübersicht*** >>](#)

- ***Jetzt scannen*** – Über diese Schaltfläche erhalten Sie standardmäßig Informationen (*Scan-Typ, Datum des letzten Scans*) zum letzten, durchgeführten Scan. Verwenden Sie den Befehl ***Jetzt scannen***, um denselben Scan erneut auszuführen, oder klicken Sie auf den Link ***Scan-Optionen***, um die Scanoberfläche von AVG zu öffnen, von der Sie Scans ausführen, planen oder Scan-Parameter bearbeiten können – siehe Kapitel [***AVG-Scans*** >>](#)

- ***Jetzt aktualisieren*** – über diesen Link erhalten Sie das Datum des letzten, durchgeführten Updatevorgangs. Klicken Sie auf diese Schaltfläche, um die Updateoberfläche zu öffnen und den Updatevorgang sofort zu starten – siehe Kapitel [***AVG Updates*** >>](#)

Auf diese Links können Sie jederzeit über die Benutzeroberfläche zugreifen. Wenn Sie einen Prozess über einen Quick Link ausführen, wechselt die GUI zu einem neuen Dialog, die Quick Links bleiben aber weiter verfügbar. Außerdem wird der ausgeführte Prozess grafisch angezeigt.

6.4. Komponentenübersicht

Der Bereich ***Sicherheitskomponenten und Statusüberblick*** befindet sich in der Mitte der [Benutzeroberfläche von AVG](#). Er ist in zwei Teile gegliedert:

- Übersicht über alle installierten Komponenten in Symbolform mit Angabe des jeweiligen Status (Aktiv oder Nicht aktiv)

- Beschreibung einer ausgewählten Komponente

In **AVG Anti-Virus 2011** enthält der Bereich ***Komponentenübersicht*** Informationen zu folgenden Komponenten:

- ***Anti-Virus*** stellt sicher, dass Ihr Computer vor Viren geschützt wird – [Details >>](#)

- ***Anti-Spyware*** gewährleistet, dass Ihr Computer vor Spyware und Adware geschützt ist –



Details >>

- ***Link Scanner*** überprüft die Suchergebnisse, die in Ihrem Internetbrowser angezeigt werden – Details >>
- ***eMail-Scanner*** überprüft alle eingehenden und ausgehenden eMails auf Viren – Details >>
- ***Residenter Schutz*** wird im Hintergrund ausgeführt und scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden – Details >>
- ***Family Safety*** unterstützt Sie beim Überwachen der Online-Aktivitäten Ihrer Kinder und schützt diese vor ungeeigneten Webinhalten – Details >>
- ***LiveKive*** bietet automatische Backups Ihrer Online-Daten – Details >>
- ***Updatemanager*** kontrolliert alle Aktualisierungen von AVG – Details >>
- ***Lizenz*** zeigt die Lizenznummer, den Lizenztyp und das Ablaufdatum an – Details >>
- ***Online Shield*** scannt alle Daten, die mit einem Webbrowser heruntergeladen werden – Details >>
- ***Anti-Rootkit*** erkennt Programme und Technologien, die darauf abzielen, Malware zu verbergen – Details >>
- ***PC Analyzer*** bietet Informationen zum Status Ihres Computers – Details >>
- ***Identitätsschutz*** – Eine Komponente für Anti-Malware, mit der Ihre persönlichen digitalen Daten vor Identitätsdiebstahl geschützt werden – Details >>
- ***Security Toolbar*** ermöglicht es Ihnen, ausgewählte Funktion von AVG direkt in Ihrem Internetbrowser zu verwenden – Details >>
- ***Remote-Verwaltung*** wird nur in AVG Business Editionen angezeigt, wenn Sie während des Installationsvorgangs angegeben haben, dass diese Komponente installiert werden soll

Klicken Sie auf eines der Komponentensymbole, um die Komponente in der Übersicht zu markieren. Im unteren Teil der Benutzeroberfläche wird eine kurze Funktionsbeschreibung der ausgewählten Komponente angezeigt. Doppelklicken Sie auf ein Symbol, um die Benutzeroberfläche der jeweiligen Komponente mit einer Auflistung von statistischen Basisdaten anzuzeigen.

Klicken Sie mit der rechten Maustaste auf das Komponentensymbol, um das Kontextmenü einzublenden: Darüber können Sie nicht nur die grafische Benutzeroberfläche der Komponente öffnen, sondern auch die Option ***Komponentenstatus ignorieren*** auswählen. Wählen Sie diese Option, wenn Ihnen bekannt ist, dass die Komponente einen Fehlerstatus aufweist, AVG aber aus einem bestimmten Grund aktiviert bleiben soll und Sie nicht durch die graue Farbe des Symbols im Infobereich gewarnt werden möchten.



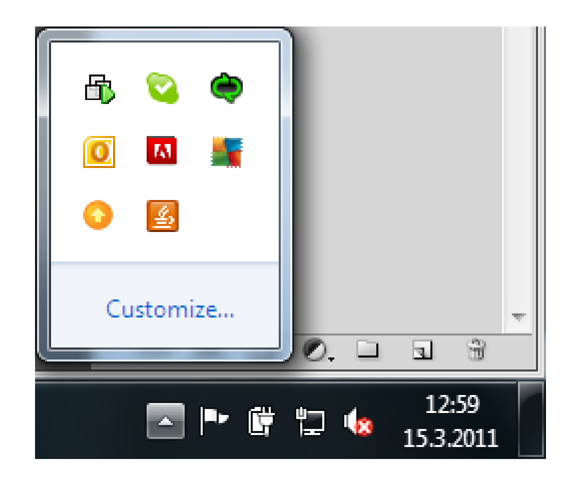
6.5. Statistik

Der Bereich ***Statistik*** befindet sich im linken, unteren Bereich der ***Benutzeroberfläche von AVG***. Dort finden Sie eine Liste von Informationen hinsichtlich der Programmvorgänge:

- ***Virendatenbank*** – Hier wird die aktuell installierte Version der Virendatenbank angegeben
- ***AVG-Version*** – Hier erhalten Sie Informationen zur installierten AVG-Version *(die Versionsnummer wird im Format 10.0.xxxx angegeben, wobei 10.0 die Version der Produktlinie ist, und xxxx für die Build-Nummer steht)*
- ***Lizenz läuft ab am:*** – Hier wird das Ablaufdatum Ihrer Lizenz von AVG angegeben

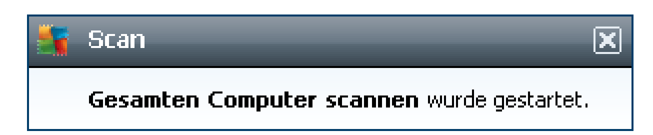
6.6. Infobereich-Symbol

Infobereichsymbol (*auf Ihrer Taskleiste von Windows*) zeigt den aktuellen Status von **AVG Anti-Virus 2011** an. Es wird immer in Ihrem Infobereich angezeigt, unabhängig davon, ob Ihr Hauptfenster von AVG geöffnet oder geschlossen ist:



Durch die Vollfarbe des ***Infobereichsymbols*** wird angezeigt, dass alle Komponenten von AVG aktiv und voll funktionsfähig sind. Das AVG-Symbol im Infobereich wird auch dann in Vollfarbe angezeigt, wenn AVG einen Fehlerstatus aufweist und Sie sich absichtlich dafür entschieden haben, den ***Komponentenstatus zu ignorieren***. Ein Symbol mit einem Ausrufezeichen zeigt an, dass ein Problem vorliegt (*inaktive Komponente, Fehlerstatus etc.*). Doppelklicken Sie auf das ***Infobereich-Symbol***, um das Hauptfenster zu öffnen und eine Komponente zu bearbeiten.

Über das Symbol im Infobereich werden Sie außerdem über laufende AVG-Prozesse und eventuelle Statusänderungen des Programms informiert (*z. B. automatischer Start eines geplanten Scans oder Updates, die Statusänderung einer Komponente, Auftreten eines Fehlerstatus, etc.*). Dabei wird über das AVG-Symbol im Infobereich ein Popup-Fenster geöffnet:





Das ***Infobereich-Symbol*** kann auch als Quick Link verwendet werden, um auf das Hauptfenster von AVG zuzugreifen. Doppelklicken Sie dazu auf das Symbol. Wenn Sie mit der rechten Maustaste auf das ***Infobereich-Symbol*** klicken, wird ein kurzes Kontextmenü mit den folgenden Optionen geöffnet:

- ***Benutzeroberfläche von AVG öffnen*** – Klicken Sie hierauf, um die Benutzeroberfläche von AVG zu öffnen
- ***Scans*** – Klicken Sie auf diese Option zum Öffnen des Kontextmenüs von
- ***PC Analyzer ausführen*** – Klicken Sie auf diese Option, um die Komponente PC Analyzer aufzurufen
- ***Scans werden durchgeführt*** – Dieser Hinweis wird nur angezeigt, wenn auf Ihrem Computer gerade ein Scan ausgeführt wird. Sie können den Scan unterbrechen, anhalten oder eine Priorität festlegen. Außerdem stehen folgenden Aktionen zur Verfügung:*Priorität für alle Scans festlegen, Alle Scans unterbrechen* oder *Alle Scans anhalten*.
- ***Jetzt aktualisieren*** – Startet ein sofortiges Update
- ***Hilfe*** – Die Hilfedatei wird auf der Startseite geöffnet

6.7. AVG-Gadget

Das ***AVG-Gadget*** wird auf dem Windows-Desktop angezeigt (*Windows-Sidebar*). Diese Anwendung wird nur in den Betriebssystemen Windows Vista und Windows 7 unterstützt. Über das ***AVG-Gadget*** können Sie direkt auf die wichtigsten Funktionen von **AVG Anti-Virus 2011** zugreifen, wie Scans und Updates:



Das ***AVG-Gadget*** bietet einen Schnellzugriff auf die folgenden Optionen:

- ***Jetzt scannen*** – Klicken Sie auf den Link ***Jetzt scannen***, um sofort einen ***Scan des gesamten Computers*** zu starten. Sie können den Scanvorgang in der geänderten Benutzeroberfläche des Gadget nachvollziehen. Eine Übersicht bietet Informationen über die Anzahl der gescannten Objekte, erkannten Bedrohungen und geheilten Bedrohungen. Sie können den Scanvorgang jederzeit unterbrechen oder anhalten. Weitere Informationen zu den Scan-Ergebnissen finden Sie im Standarddialog ***Übersicht über Scan-Ergebnisse*** , der direkt vom Gadget aus über die Option ***Details anzeigen*** geöffnet werden kann (die entsprechenden Scan-Ergebnisse werden unter ***Scan der Sidebar-***



Gadgets aufgelistet).



- ***Jetzt aktualisieren*** – Klicken Sie auf ***Jetzt aktualisieren***, um das AVG-Update direkt über das Gadget zu starten:



- ***Twitter-Link*** – Öffnet eine neue Benutzeroberfläche des ***AVG-Gadget*** mit einer Übersicht über die neuesten Twitter-Feeds zu AVG. Klicken Sie auf den Link ***Alle Twitter-Feeds von AVG anzeigen***, um die speziell auf AVG bezogene Twitter-Website in einem neuen Fenster Ihres Internetbrowsers zu öffnen:



- ***Facebook-Link*** – Öffnet in Ihrem Internetbrowser die Seite der ***AVG Community*** auf Facebook



- ***LinkedIn*** – Diese Option ist nur innerhalb der Netzwerkinstallation verfügbar (*d. h. vorausgesetzt, dass AVG mit einer Lizenz für AVG Business Edition installiert wurde*) und öffnet Ihren Internet-Browser mit der Website ***AVG SMB Community*** des sozialen Netzwerks „LinkedIn“

- ***PC Analyzer*** –·Öffnet die Benutzeroberfläche in der Komponente ***PC Analyzer***

- ***Suchfeld*** – Geben Sie ein Schlüsselwort ein, und Sie erhalten die Suchergebnisse sofort in einem neu geöffneten Fenster Ihres Standardwebbrowsers



7. Komponenten von AVG

7.1. Anti-Virus

7.1.1. Grundlagen zu Anti-Virus

Die Scan-Engine der Antivirensoftware überprüft alle Dateien und Dateiaktivitäten (Öffnen/Schließen von Dateien usw.) auf bekannte Viren. Alle erkannten Viren werden blockiert, so dass sie keine Aktionen ausführen können, und anschließend bereinigt oder in die Quarantäne verschoben. Die meisten Antivirenprodukte verwenden auch einen heuristischen Scan, mit dem Dateien auf typische Virenmerkmale (sogenannte Virensignaturen) überprüft werden. Auf diese Weise kann der Antivirenscanner neue, unbekannte Viren erkennen, wenn diese typische Merkmale eines vorhandenen Virus aufweisen.

Die wichtigste Funktion des Virenschutzes ist, sicherzustellen, dass keine bekannten Viren auf dem Computer ausgeführt werden können!

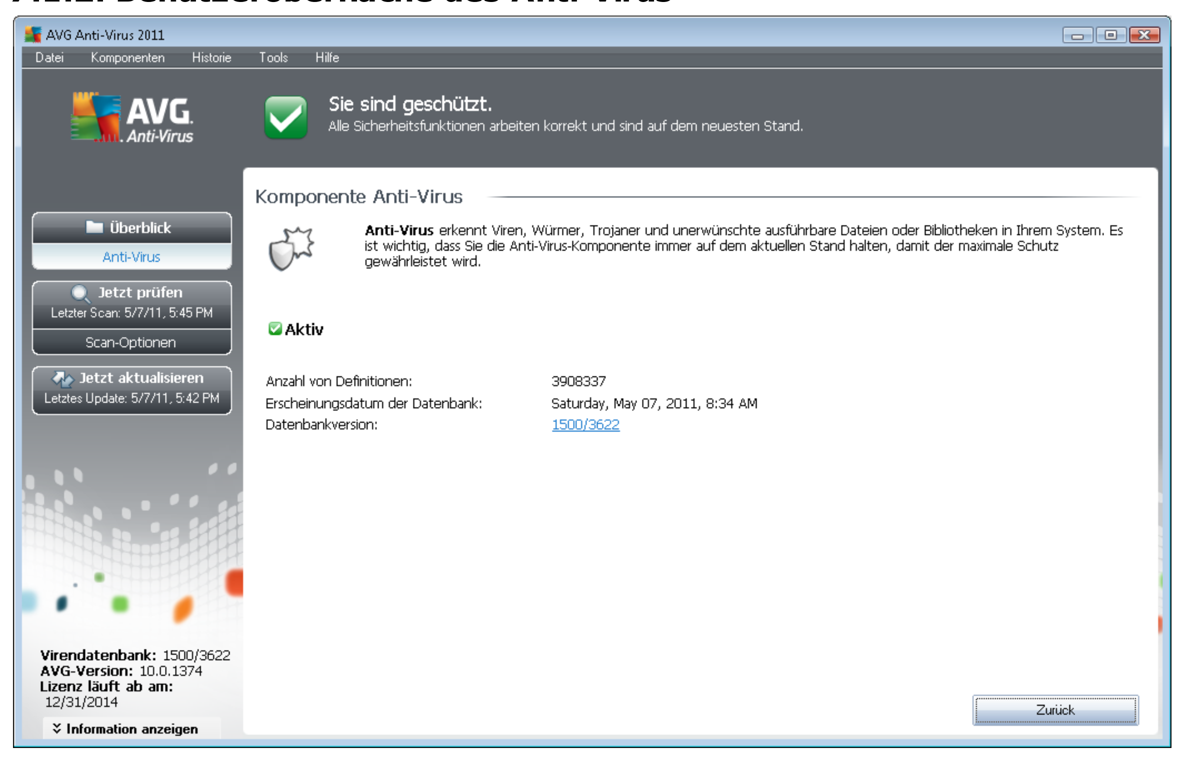
Während eine einzige Technologie häufig nicht in der Lage ist, alle Viren zu erkennen oder zu identifizieren, gewährleistet ***Anti-Virus*** durch Kombination mehrerer Technologien einen umfassenden Schutz des Computers:

- Scannen – Die Suche nach Zeichenfolgen, die charakteristisch für ein bestimmtes Virus sind
- Heuristische Analyse – Dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung
- Generische Erkennung – Erkennung von Anweisungen, die typisch für ein bestimmtes Virus oder eine Gruppe von Viren sind

AVG kann zudem im System unerwünschte ausführbare Anwendungen oder DLL-Bibliotheken analysieren und erkennen. Diese Bedrohungen bezeichnen wir als potentiell unerwünschte Programme (verschiedene Arten von Spyware, Adware usw.). Außerdem durchsucht AVG Ihre System-Registry nach verdächtigen Einträgen, temporären Internetdateien und Tracking Cookies und ermöglicht Ihnen, alle potentiell schädlichen Elemente wie jegliche andere Infektion zu behandeln.



7.1.2. Benutzeroberfläche des Anti-Virus



Die Benutzeroberfläche von ***Anti-Virus*** enthält grundlegende Informationen zur Funktionalität der Komponente und zum aktuellen Status (*Die Komponente Anti-Virus ist aktiv*) sowie eine Übersicht über statistische Daten zu ***Anti-Virus***:

- ***Anzahl von Definitionen*** – Anzahl der in der aktuellen Version der Virendatenbank definierten Viren
- ***Erscheinungsdatum der Datenbank*** – Datum und Uhrzeit des letzten Updates der Viren-Datenbank
- ***Datenbankversion*** – Versionsnummer der aktuell installierten Virendatenbank; wird bei jedem Update der Virendatenbank erhöht

Die Benutzeroberfläche der Komponente enthält nur eine Schaltfläche (***Zurück***), mit der Sie zum Hauptfenster der Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückkehren können.

7.2. Anti-Spyware

7.2.1. Grundlagen zu Anti-Spyware

Spyware wird normalerweise als eine Art Malware definiert, d. h. Software, die ohne Wissen und Zustimmung des Benutzers Informationen auf dem Computer sammelt. Einige Spyware-Programme können bewusst installiert werden und enthalten häufig Werbung, Popup-Fenster oder ähnlich

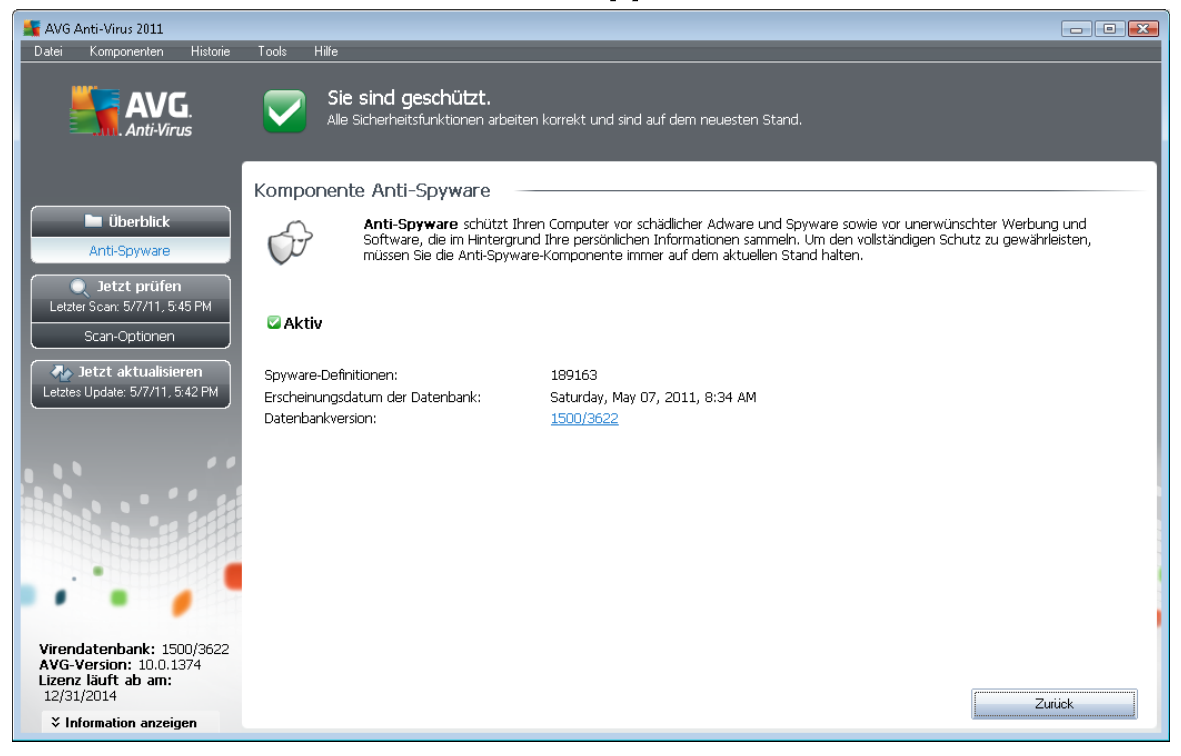


unerfreuliche Software.

Derzeit geht die größte Infektionsgefahr von Websites mit potentiell gefährlichen Inhalten aus. Jedoch ist auch eine Übertragung per eMail oder durch Würmer und Viren eine durchaus gängige Infektionsmöglichkeit. Der wichtigste Schutz ist ein Scanner, der ständig im Hintergrund ausgeführt wird, wie z. B. die Komponente ***Anti-Spyware***, die wie ein residenter Schutz funktioniert und Ihre Anwendungen während der Arbeit im Hintergrund überprüft.

Es ist allerdings möglich, dass Malware bereits vor der Installation von AVG auf den Computer übertragen wurde oder dass Sie **AVG Anti-Virus 2011** nicht mit den neuesten Datenbank- und Programmaktualisierungen ausgestattet haben. Daher können Sie mit AVG Ihren Computer mithilfe der Scan-Funktion vollständig auf Malware bzw. Spyware überprüfen. Außerdem erkennt die Komponente ruhende und nicht aktive Malware, d. h. Malware, die heruntergeladen, aber noch nicht aktiviert wurde.

7.2.2. Benutzeroberfläche der Anti-Spyware



Die Benutzeroberfläche von ***Anti-Spyware*** enthält eine Übersicht über die Funktionsweise der Komponente, Informationen zum aktuellen Status sowie einige Statistiken zu ***Anti-Spyware***:

- ***Spyware-Definitionen*** – Anzahl der in der neuesten Spyware-Datenbankversion definierten Spyware-Muster
- ***Erscheinungsdatum der Datenbank*** – Datum und Uhrzeit des letzten Updates der Spyware-Datenbank
- ***Datenbankversion*** – Versionsnummer der aktuellsten Spyware-Datenbank; wird bei jeder Aktualisierung der Virendatenbank erhöht



Die Benutzeroberfläche der Komponente enthält nur eine Schaltfläche (***Zurück***), mit der Sie zum Hauptfenster der Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückkehren können.

7.3. Link Scanner

7.3.1. Grundlagen zum Link Scanner

Link Scanner schützt vor den akuten kurzlebigen Bedrohungen aus dem Internet. Gefahren lauern auf allen möglichen Webseiten, egal ob es sich um Seiten von Regierungsbehörden, großen und bekannten Markenfirmen oder Kleinbetrieben handelt. Und sie verweilen dort selten länger als 24 Stunden. ***Link Scanner*** sorgt für den nötigen Schutz durch Analyse aller sich hinter einem Link verbergenden Webseiten. Das garantiert den gewünschten Schutz im entscheidenden Moment: nämlich kurz bevor Sie auf den Link klicken.

Die Technologie von ***Link Scanner*** umfasst zwei Hauptbestandteile: ***Search-Shield*** und ***Surf-Shield***:

- ***Search-Shield*** enthält eine Liste von Websites (*URL-Adressen*), deren Gefährlichkeit bekannt ist. Wenn Sie eine Internetsuche mit Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg oder SlashDot durchführen, werden alle Suchergebnisse gemäß dieser Liste überprüft. Jedes Ergebnis erhält anschließend ein Zertifikatssymbol (*für Suchergebnisse von Yahoo wird nur das Zertifikatssymbol für „ausgewertete Website" angezeigt*).

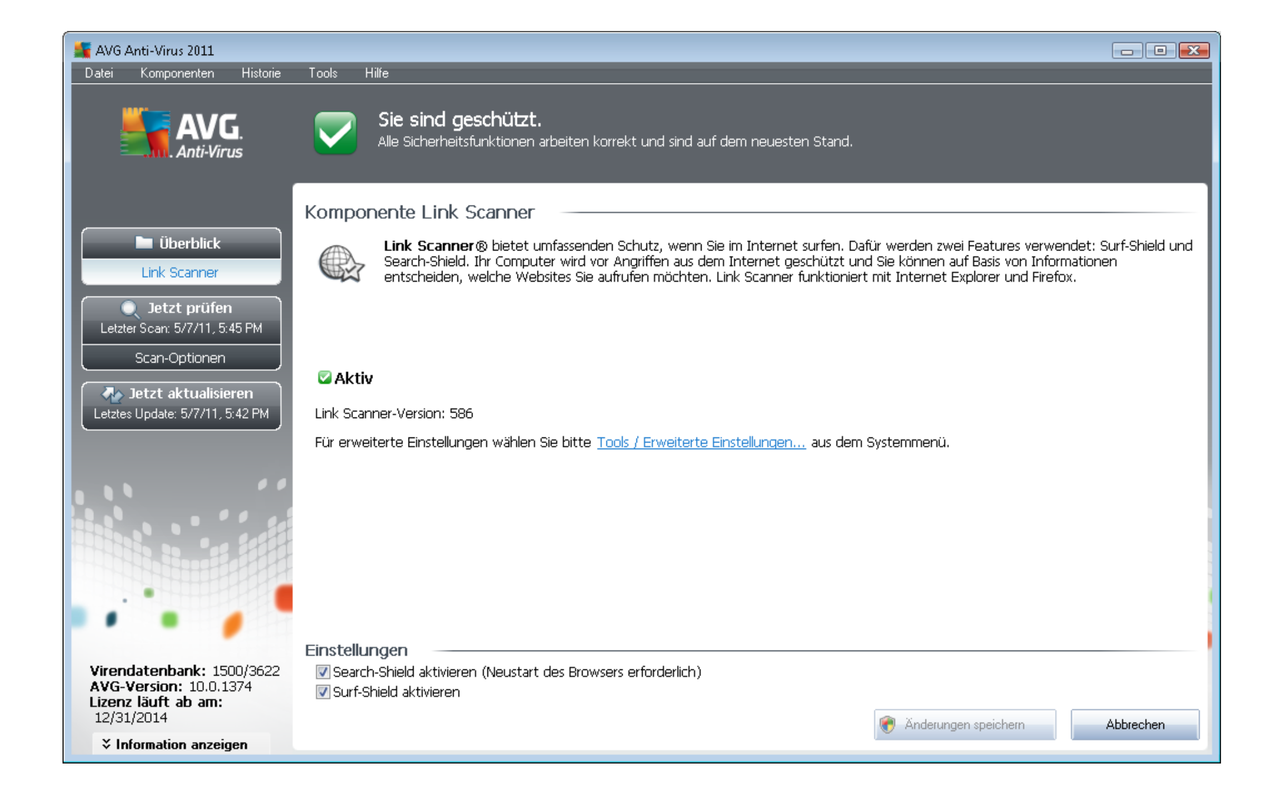
- ***Surf-Shield***scannt die Inhalte der von Ihnen besuchten Websites unabhängig von deren Adresse. Selbst wenn eine Website nicht von ***Search-Shield*** erkannt wird (*z. B. wenn eine neue verseuchte Website erstellt wird oder wenn eine bisher saubere Website jetzt Malware enthält*), wird diese von ***Surf-Shield*** erkannt und blockiert, sobald Sie versuchen, die Website aufzurufen.

Hinweis: *Link Scanner ist nicht für Serverplattformen vorgesehen.*

7.3.2. Benutzeroberfläche des Link Scanners

Die Benutzeroberfläche von ***Link Scanner*** umfasst eine kurze Beschreibung der Funktionen der Komponente sowie Informationen über ihren aktuellen Status. Darüber hinaus können Sie die neueste Versionsnummer der ***Link Scanner*** -Datenbank (*Link Scanner-Version) abrufen.*





Einstellungen von Link Scanner

Im unteren Bereich des Dialogs können Sie verschiedene Optionen bearbeiten:

- ***Search-Shield***aktivieren – (*standardmäßig aktiviert*): Benachrichtigungssymbole zu Suchabfragen in Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg und SlashDot: Die Symbole weisen darauf hin, dass der Inhalt der als Suchergebnis angezeigten Sites überprüft wurde.

- ***Surf-Shield*** aktivieren – (*standardmäßig aktiviert*): Aktiver (*Echtzeit*-) Schutz vor unbeabsichtigtem Zugriff auf Exploit-Sites. Die Verbindungsherstellung zu bekannten bösartigen Sites und deren schädlichem Inhalt wird blockiert, wenn der Benutzer diese Sites über einen Webbrowser (*oder eine andere HTTP-basierte Anwendung*) aufruft.

7.3.3. Search-Shield

Wenn das Internet mit aktiviertem ***Search-Shield*** durchsucht wird, werden alle angezeigten Suchergebnisse der bekanntesten Suchmaschinen (*Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg und SlashDot*) auf gefährliche oder verdächtige Links hin untersucht. Da ***AVG Link Scanner*** diese Links überprüft und gefährliche Links entsprechend markiert, werden Sie gewarnt, bevor Sie auf solche Links klicken. So können Sie sicherstellen, dass Sie ausschließlich sichere Websites aufrufen.

Während ein Link auf der Seite mit den Suchergebnissen überprüft wird, weist ein Symbol neben dem Link auf diese laufende Überprüfung hin. Sobald die Bewertung abgeschlossen ist, wird das entsprechende Informationssymbol angezeigt:



Die verlinkte Seite ist sicher (*dieses Symbol wird nicht bei sicheren Suchergebnissen von Yahoo! JP angezeigt*).

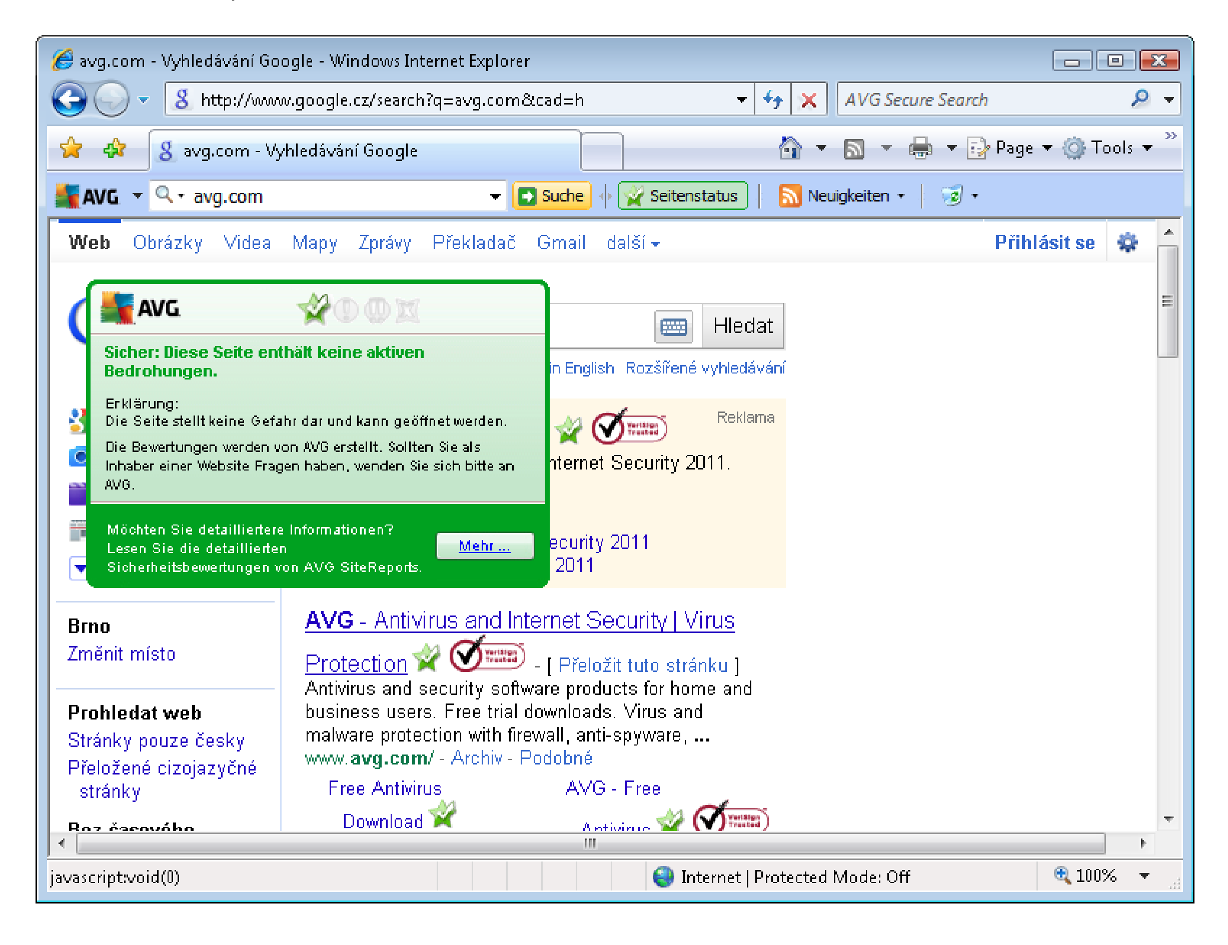
Die verlinkte Seite enthält keine Bedrohungen, wird aber als verdächtig eingestuft (*die Herkunft/der Zweck der Seite ist fragwürdig, weshalb von Online-Einkäufen abgeraten wird usw.*).

Die verlinkte Seite stellt momentan kein Sicherheitsrisiko dar, kann aber Links zu eindeutig gefährlichen Seiten oder verdächtigen Code enthalten.

Die verlinkte Seite enthält aktive Bedrohungen! Aus Sicherheitsgründen können Sie nicht auf diese Seite zugreifen.

Auf die verlinkte Seite kann nicht zugegriffen werden. Darum konnte sie auch nicht gescannt werden.

Wenn Sie mit der Maus über ein bestimmtes Bewertungssymbol fahren, werden Details zu dem entsprechenden Link angezeigt. Zu den Informationen gehören Details über die Art der Gefahr (*sofern vorhanden*):

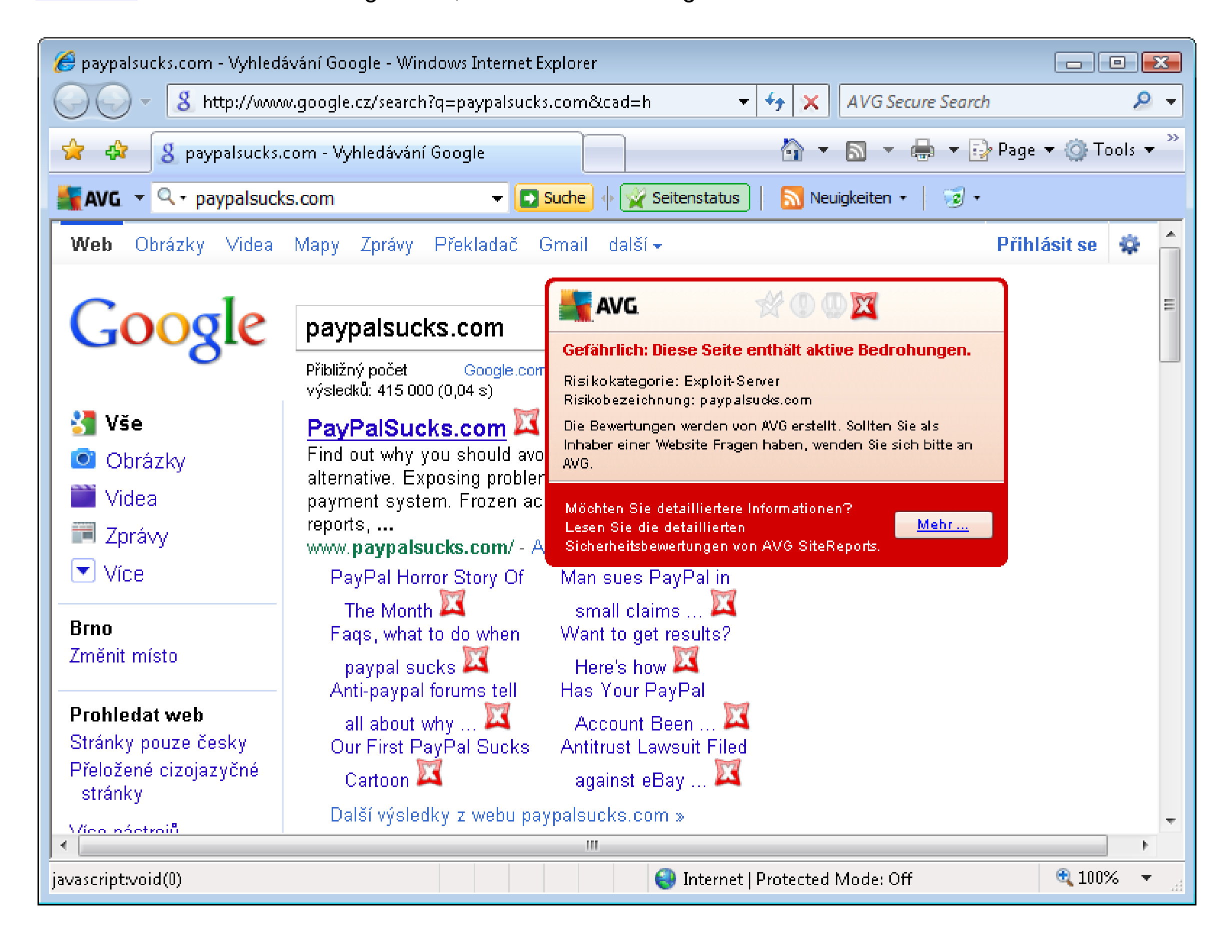




7.3.4. Surf-Shield

Diese leistungsfähige Schutzfunktion sorgt dafür, dass bösartige Inhalte von jeder Webseite, die Sie öffnen möchten, blockiert und nicht auf Ihren Computer heruntergeladen werden können. Wenn diese Funktion aktiviert ist und Sie auf einen gefährlichen Link klicken oder die Internetadresse einer gefährlichen Site eingeben, wird die entsprechende Webseite automatisch blockiert, damit sich Ihr Computer nicht infiziert. Denken Sie daran, dass Website-Exploits Ihren Computer bereits infizieren können, wenn Sie einfach nur die entsprechende Site besuchen. Wenn Sie versuchen, auf eine gefährliche Webseite mit Exploits oder anderen ernsthaften Bedrohungen zuzugreifen, hält ***AVG Link Scanner*** Ihren Browser davon ab, die Seite zu öffnen.

Wenn Sie in Ihrem Webbrowser auf eine gefährliche Website stoßen, werden Sie von ***AVG Link Scanner*** mit einem Fenster gewarnt, das in etwa wie folgt aussieht:



Der Aufruf einer solchen Website ist äußerst gefährlich und wird nicht empfohlen!

7.4. Residenter Schutz



7.4.1. Grundlagen zu Residenter Schutz

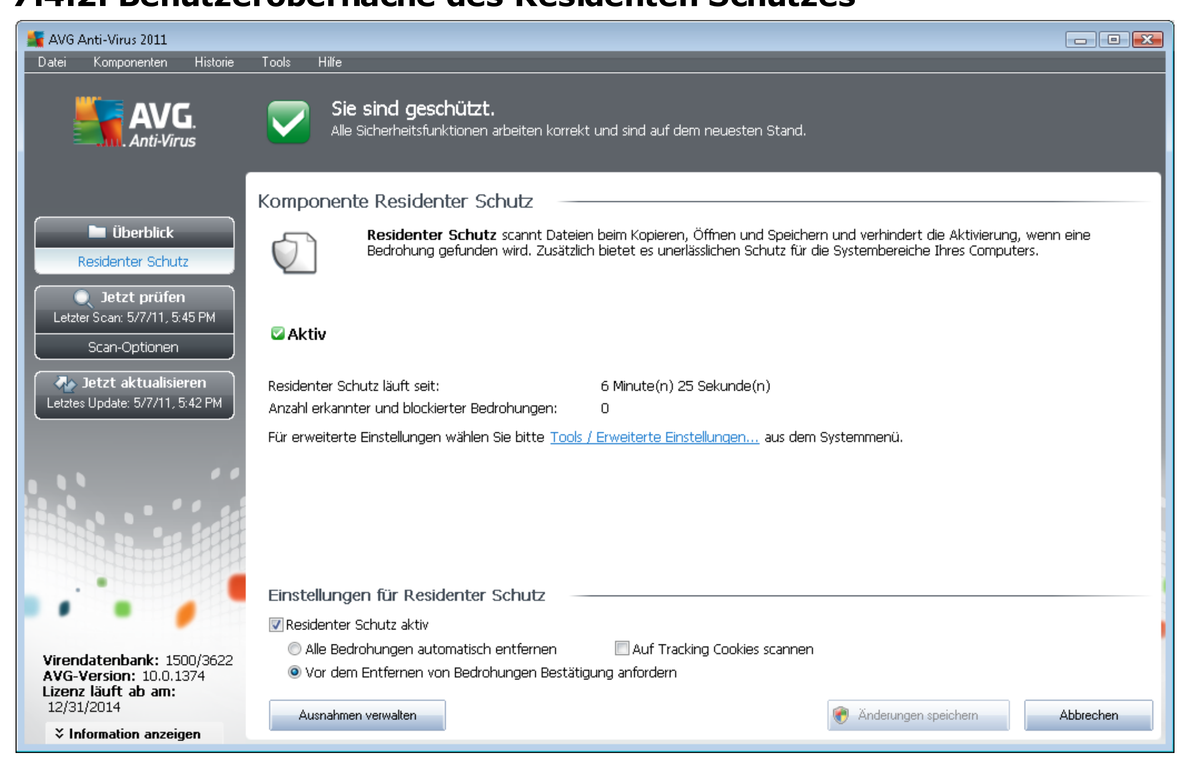
Die Komponente ***Residenter Schutz*** gewährt Ihrem Computer dauerhaften Schutz. Sie scannt jede einzelne Datei, die geöffnet, gespeichert oder kopiert wird und überwacht die Systembereiche Ihres Computers. Wenn der ***Residente Schutz*** in einer Datei, auf die zugegriffen wird, ein Virus entdeckt, stoppt die Komponente den aktuell ausgeführten Vorgang und gestattet es dem Virus nicht, sich zu aktivieren. Normalerweise nehmen Sie diesen Vorgang nicht wahr, da er „im Hintergrund" abläuft und Sie nur informiert werden, wenn Bedrohungen gefunden werden; gleichzeitig blockiert der ***Residente Schutz*** die Aktivierung der Bedrohung und entfernt sie. Der ***Residente Schutz*** wird beim Systemstart in den Speicher Ihres Computers geladen.

Aufgaben des Residenten Schutzes

- Scannen auf bestimmte mögliche Bedrohungen
- Scannen von Wechseldatenträgern (*Flash-Disks usw.*)
- Scannen von Dateien mit bestimmten Erweiterungen oder Dateien ohne Erweiterungen
- Festlegen von Ausnahmen für Scans (bestimmte Dateien oder Ordner, die nie gescannt werden sollen)

Warnung: Der Residente Schutz wird beim Systemstart in den Speicher Ihres Computers geladen. Sie sollten den Schutz in keinem Fall deaktivieren!

7.4.2. Benutzeroberfläche des Residenten Schutzes



Neben einer Übersicht über die Funktionen des ***Residenten Schutzes*** und Informationen zum Status



der Komponente enthält die Benutzeroberfläche des ***Residenten Schutzes*** auch einige statistische Daten:

- ***Residenter Schutz läuft seit*** – Abgelaufene Zeit seit dem letzten Start der Komponenten
- ***Anzahl erkannter und blockierter Bedrohungen*** – Anzahl der erkannten Infektionen, deren Ausführung/Öffnen verhindert wurde (*wenn nötig kann dieser Wert zurückgesetzt werden, z. B. für statistische Zwecke – Wert zurücksetzen*)

Einstellungen für Residenter Schutz

Im unteren Teil des Dialogs befindet sich der Bereich ***Einstellungen für Residenter Schutz***, in dem Sie einige Basiseinstellungen für die Funktionsweise der Komponente bearbeiten können (*eine detaillierte Konfiguration ist, wie bei allen anderen Komponenten, über die Option „Tools"/„Erweiterte Einstellungen" des Systemmenüs möglich*).

Über die Option ***Residenter Schutz aktiv*** können Sie den Residenten Schutz einfach ein- und ausschalten. Standardmäßig ist die Funktion aktiviert. Mit dem Residenten Schutz können Sie zudem festlegen, wie erkannte Infektionen behandelt (entfernt) werden sollen:

- o entweder automatisch (***Alle Bedrohungen automatisch entfernen***)
- o oder erst nach Bestätigung durch den Benutzer (***Vor dem Entfernen von Bedrohungen Bestätigung anfordern***)

Diese Auswahl hat keinen Einfluss auf die Sicherheitsstufe und kann beliebig festgelegt werden.

In beiden Fällen können Sie die Option ***Auf Tracking Cookies scannen*** auswählen. In bestimmten Fällen kann es sinnvoll sein, diese Option zu aktivieren, um maximale Sicherheit zu erzielen, sie ist jedoch standardmäßig deaktiviert. (*Cookies = Textpakete, die von einem Server an einen Webbrowser gesendet und dann bei jedem Zugriff des Browsers auf diesen Server unverändert vom Browser zurückgesendet werden. HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

Hinweis: Alle *Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü den Eintrag* ***Tools / Erweiterte Einstellungen*** *aus, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

Auf der Oberfläche des ***Residenten Schutzes*** stehen folgende Schaltflächen zur Verfügung:

- ***Ausnahmen verwalten*** – Öffnet den Dialog ***Residenter Schutz – Ausgeschlossene Einträge***, in dem Sie Ordner und Dateien festlegen können, die vom ***Residenten Schutz*** nicht durchsucht werden sollen



- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren

7.4.3. Erkennungen durch den Residenten Schutz

Residenter Schutz scannt Dateien, wenn diese kopiert, geöffnet oder gespeichert werden. Wenn ein Virus oder eine andere Bedrohung erkannt wird, werden Sie unmittelbar mit folgendem Dialog gewarnt:



In diesem Warndialog finden Sie Informationen zu der Datei, die als infiziert erkannt wurde (*Dateiname*), den Namen der erkannten Bedrohung (*Name der Bedrohung*) und einen Link zur ***Virenenzyklopädie***, wo Sie weitere Informationen zur erkannten Infektion finden, falls bekannt (*Weitere Informationen*).

Zudem müssen Sie die erforderliche Aktion auswählen – die folgenden Optionen stehen zur Verfügung:

Beachten Sie, dass unter bestimmten Bedingungen (Art und Speicherort der infizierten Datei) nicht immer alle Optionen verfügbar sind.

- ***Bedrohung als Hauptbenutzer entfernen*** – Aktivieren Sie das Kontrollkästchen, falls Sie der Meinung sind, dass Sie als normaler Benutzer nicht genügend Rechte zum Entfernen der Datei haben. Hauptbenutzer verfügen über umfassende Zugriffsrechte. Falls sich die Bedrohung·in einem bestimmten Systemordner befindet, müssten Sie, wenn nötig, das Kontrollkästchen für ein erfolgreiches Entfernen aktivieren.

- ***Heilen*** – Diese Schaltfläche wird nur angezeigt, wenn die erkannte Infektion geheilt werden kann. Daraufhin wird die Infektion aus der Datei entfernt, und der ursprüngliche Zustand der Datei wird wiederhergestellt. Wenn es sich bei der Datei selbst um einen Virus handelt, verwenden Sie diese Schaltfläche, um sie zu löschen (*d. h. in die **Virenquarantäne***



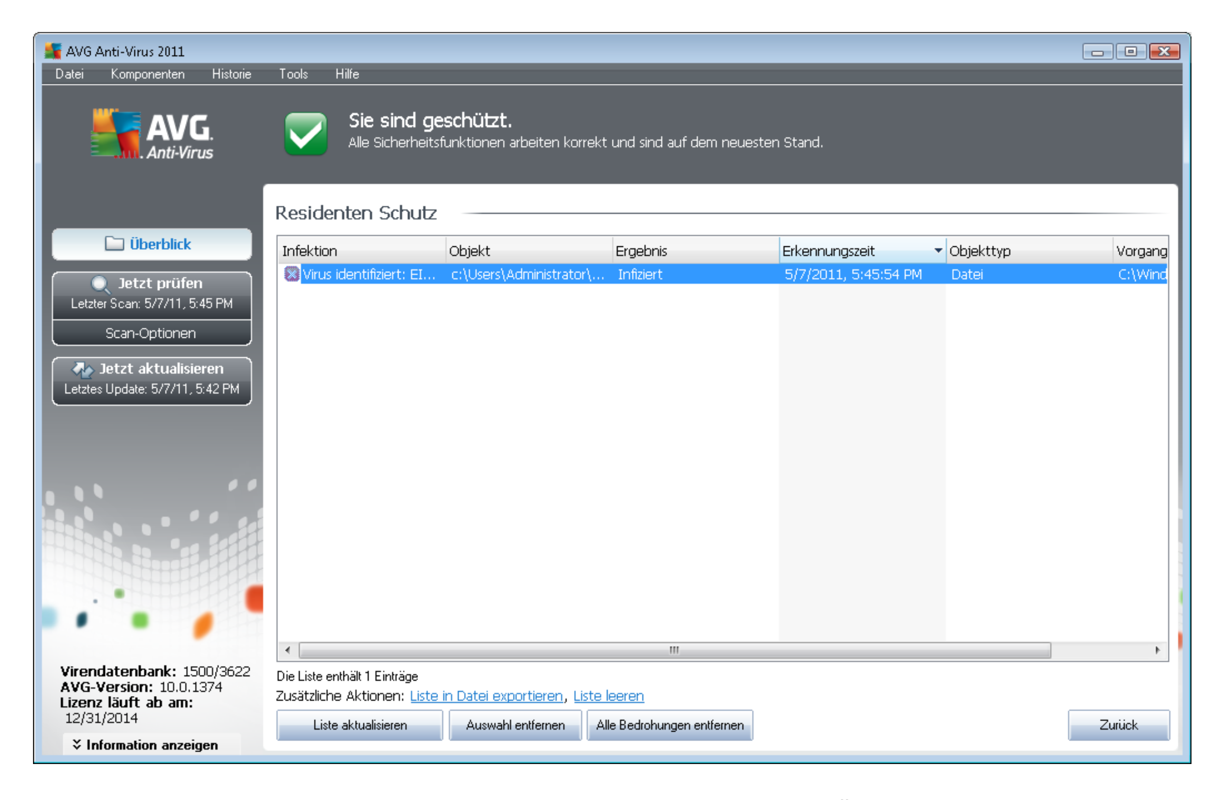
verschieben)

- ***In Quarantäne verschieben*** – Der Virus wird in die AVG-***Virenquarantäne verschoben***
- ***Gehe zu Datei*** – Mit dieser Option werden Sie zum genauen Speicherort des verdächtigen Objekts weitergeleitet (*öffnet ein neues Fenster von Windows Explorer*)
- ***Ignorieren*** – Es wird dringend empfohlen, diese Option NICHT zu verwenden, wenn Sie keinen wirklich guten Grund dazu haben!

Hinweis: *Die Größe des entdeckten Objektes kann gegebenenfalls den verfügbaren Speicherplatz der Virenquarantäne überschreiten. In diesem Fall erscheint eine Warnmeldung, die Sie über das Problem informiert, wenn Sie versuchen, das infizierte Objekt in die Quarantäne zu verschieben. Die Größe des Quarantänespeichers kann jedoch angepasst werden. Sie ist als einstellbarer Prozentsatz der tatsächlichen Größe Ihrer Festplatte definiert. Um die Größe Ihres Quarantänespeichers zu erhöhen, rufen Sie den Quarantäne-Dialog innerhalb der Erweiterten Einstellungen für AVG auf und ändern Sie die Option 'Größe der Quarantäne begrenzen'.*

Im unteren Abschnitt des Dialogs finden Sie den Link ***Details anzeigen*** – Klicken Sie auf diesen Link, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess zu öffnen, der beim Erkennen der Infektion ausgeführt wurde.

Die Gesamtübersicht über alle vom ***Residenten Schutz*** gefundenen Bedrohungen können Sie im Dialog ***Erkennung durch den Residenten Schutz*** aufrufen, und zwar im Systemmenü unter der Option ***Historie/Ergebnisse des Residenten Schutzes***:



Der Bereich ***Erkennung durch den Residenten Schutz*** enthält eine Übersicht über Objekte, die



durch den ***Residenten Schutz*** erkannt, als gefährlich bewertet und entweder geheilt oder in die ***Virenquarantäne*** verschoben wurden. Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Infektion*** – Beschreibung (nach Möglichkeit auch Name) des erkannten Objekts
- ***Objekt*** - Speicherort des Objekts
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Der Zeitpunkt (Datum und Uhrzeit), zu dem das verdächtige Objekt entdeckt wurde
- ***Objekttyp*** - Typ des erkannten Objekts
- ***Vorgang*** - Ausgeführte Aktion, mit der das potentiell gefährliche Objekt aufgerufen wurde, so dass es erkannt werden konnte

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei exportieren***) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***). Die Schaltfläche ***Liste aktualisieren*** aktualisiert die Liste der vom ***Residenten Schutz*** erkannten Funde. Mit der Schaltfläche ***Zurück*** können Sie zurHauptseite der ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren.

7.5. Family Safety

AVG Family Safety unterstützt Sie beim Schutz Ihrer Kinder vor unangemessenen Websites, Medieninhalten und Online-Suchergebnissen und bietet Ihnen Berichte zu ihren Online-Aktivitäten. Sie können für jedes Ihrer Kinder die angemessene Schutzstufe einstellen und sie einzeln über eindeutige Anmeldedaten überwachen.

Die Komponente ist nur aktiv, wenn das Produkt ***AVG Family Safety*** auf Ihrem Computer installiert ist. Wenn ***AVG Family Safety*** nicht installiert ist, klicken Sie auf das zugehörige Symbol innerhalb der Benutzerschnittstelle von **AVG Anti-Virus 2011** und Sie werden auf die Produkt-Website geleitet, auf der Sie die erforderlichen Informationen finden.

7.6. AVG LiveKive

AVG LiveKive sichert automatisch Ihre gesamten Dateien, Fotos und Musik an einem sicheren Ort und ermöglicht es Ihnen, diese mit Ihrer Familie und Ihren Freunden gemeinsam zu nutzen. Sie haben von allen internetfähigen Geräten, einschließlich iPhones und Android-Geräten, Zugriff auf diese.

Die Komponente ist nur aktiv, wenn das Produkt ***AVG LiveKive*** auf Ihrem Computer installiert ist. Wenn Sie das Produkt ***AVG LiveKive*** nicht installiert haben, klicken Sie auf das entsprechende Symbol innerhalb der Benutzerschnittstelle von **AVG Anti-Virus 2011** , und Sie werden auf die Produktwebsite geleitet, auf der Sie alle erforderlichen Informationen finden.



7.7. eMail-Scanner

eMails sind eine der häufigsten Quellen von Viren und Trojanern. eMail-Nachrichten können jedoch in Form von Phishing und Spam auch noch andere Risiken in sich bergen. Kostenlose eMail-Konten sind häufiger solchen schädlichen eMails ausgesetzt (*da nur selten Technologie für Anti-Spam eingesetzt wird*); solche Konten werden vor allem von privaten Benutzer verwendet. Durch das Aufsuchen unbekannter Websites sowie das Ausfüllen von Online-Formularen mit persönlichen Daten (*inklusive eMail-Adresse*) erhöht sich für private Benutzer das Risiko, Opfer eines Angriffs via eMail zu werden. Unternehmen nutzen in der Regel eigene eMail-Konten und verwenden Anti-Spam-Filter, um die beschriebenen Risiken zu minimieren.

7.7.1. Grundlagen zum eMail-Scanner

Der ***Personal eMail-Scanner*** prüft eingehende und ausgehende eMails automatisch. Sie können ihn für eMail-Clients verwenden, die über kein eigenes Plugin in AVG verfügen (*kann aber auch zum Scannen von eMails für eMail-Clients verwendet werden, die von AVG mit einem bestimmten Plugin unterstützt werden, z. B. Microsoft Outlook und The Bat*). Der eMail-Scanner ist hauptsächlich für die Verwendung mit Anwendungen wie Outlook Express, Mozilla, Incredimail usw. vorgesehen.

Während der Installation von AVG werden für die Prüfung der eMails automatische Server eingerichtet: einer für die Prüfung eingehender eMails und einer für die Prüfung ausgehender eMails. Mithilfe dieser beiden Server werden eMails an den Ports 110 und 25 (*den Standardports für das Senden/Empfangen von eMails*) automatisch überprüft.

eMail-Scanner fungiert als Schnittstelle zwischen dem jeweiligen eMail-Client und eMail-Servern im Internet.

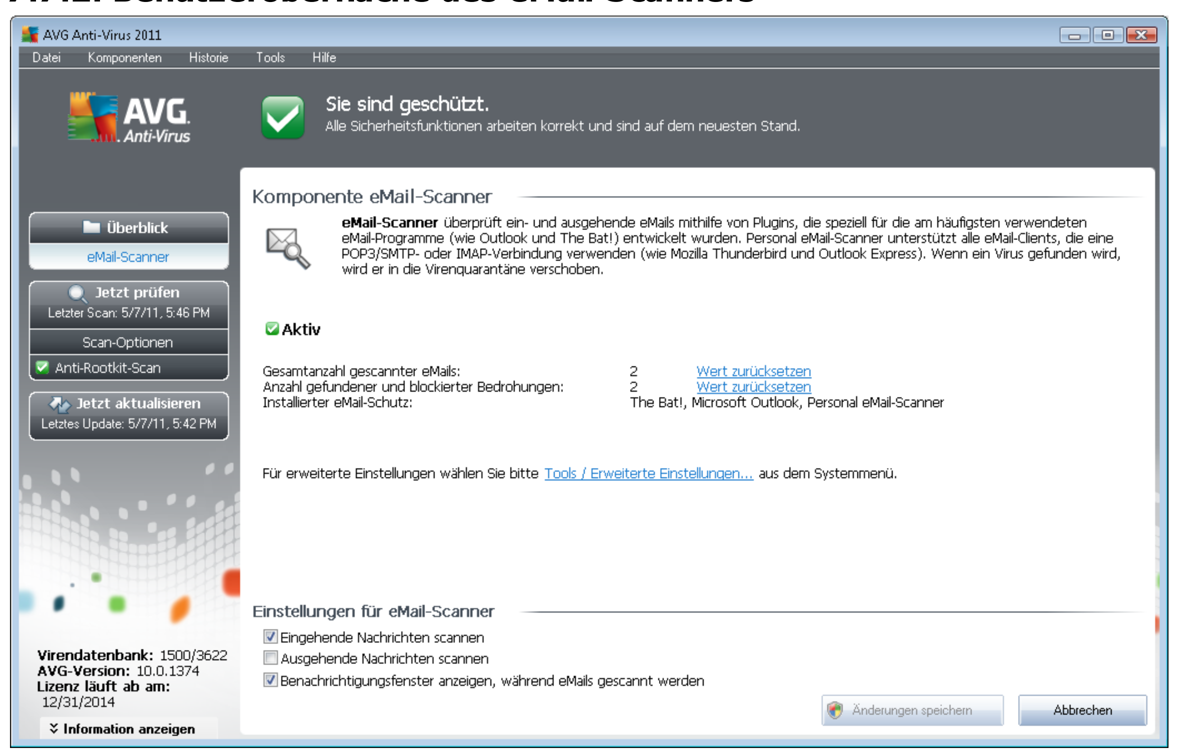
- ***Eingehende eMail:*** Beim Empfang einer eMail vom Server prüft die Komponente ***eMail-Scanner*** die Nachricht auf Viren, entfernt infizierte Anhänge und fügt eine Zertifizierung hinzu. Sobald ein Virus erkannt wird, wird es umgehend in die ***Virenquarantäne*** verschoben. Dann wird die Nachricht an den eMail-Client übergeben.

- ***Ausgehende eMail:*** Die Nachricht wird vom eMail-Client an eMail-Scanner gesendet; dieser prüft die Nachricht mitsamt Anhängen auf Viren und leitet die eMail an den SMTP-Server weiter (*die Prüfung ausgehender eMails ist standardmäßig deaktiviert, kann jedoch manuell aktiviert werden*).

Hinweis: *AVG eMail-Scanner ist nicht für Serverplattformen vorgesehen!*



7.7.2. Benutzeroberfläche des eMail-Scanners



Der Dialog der Komponente ***eMail-Scanner*** enthält eine kurze Beschreibung der Funktionsweise der Komponente, Informationen zum aktuellen Status sowie die folgenden Statistiken:

- ***Gesamtanzahl gescannter eMails*** – Anzahl der eMails, die seit dem letzten Start des ***eMail-Scanners*** gescannt wurden (*dieser Wert kann bei Bedarf zurückgesetzt werden; z. B. aus statistischen Gründen – Wert zurücksetzen*)

- ***Anzahl gefundener und blockierter Bedrohungen*** – Anzahl der Infektionen, die seit dem letzten Start des ***eMail-Scanners*** in eMail-Nachrichten gefunden wurden

- ***Installierter eMail-Schutz*** – Informationen zu einem bestimmten eMail-Schutz-Plugin bezüglich Ihres installierten Standard-eMail-Clients

Einstellungen für den eMail-Scanner

Im unteren Teil des Dialogs befindet sich der Bereich ***Einstellungen für eMail-Scanner***, in dem Sie einige Grundfunktionen der Komponente bearbeiten können:

- ***Eingehende Nachrichten scannen*** – Aktivieren Sie diesen Eintrag, damit alle in Ihrem Konto eingehenden eMails auf Viren überprüft werden. Dieser Eintrag ist standardmäßig aktiviert, und wir empfehlen Ihnen ausdrücklich, diese Einstellung nicht zu ändern!

- ***Ausgehende Nachrichten scannen*** – Markieren Sie diesen Eintrag, damit alle eMails, die von Ihrem Konto gesendet werden, auf Viren geprüft werden. Standardmäßig ist dieser



Eintrag deaktiviert.

- ***Benachrichtigungsfenster anzeigen, während eMails gescannt werden*** – Aktivieren Sie diesen Eintrag, wenn Sie beim Scannen Ihrer eMails mit der Komponente ***eMail-Scanner*** über den Benachrichtigungsdialog, der über dem AVG-Symbol im Infobereich angezeigt wird, benachrichtigt werden möchten. Dieser Eintrag ist standardmäßig aktiviert, und wir empfehlen Ihnen ausdrücklich, diese Einstellung nicht zu ändern!

Eine erweiterte Konfiguration der Komponente ***eMail-Scanner*** kann über das Systemmenü mit den Optionen ***Tools/Erweiterte Einstellungen*** durchgeführt werden. Die erweiterte Konfiguration sollte jedoch nur von erfahrenen Benutzern verwendet werden!

Hinweis:*Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü den Eintrag* ***Tools / Erweiterte Einstellungen*** *aus, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

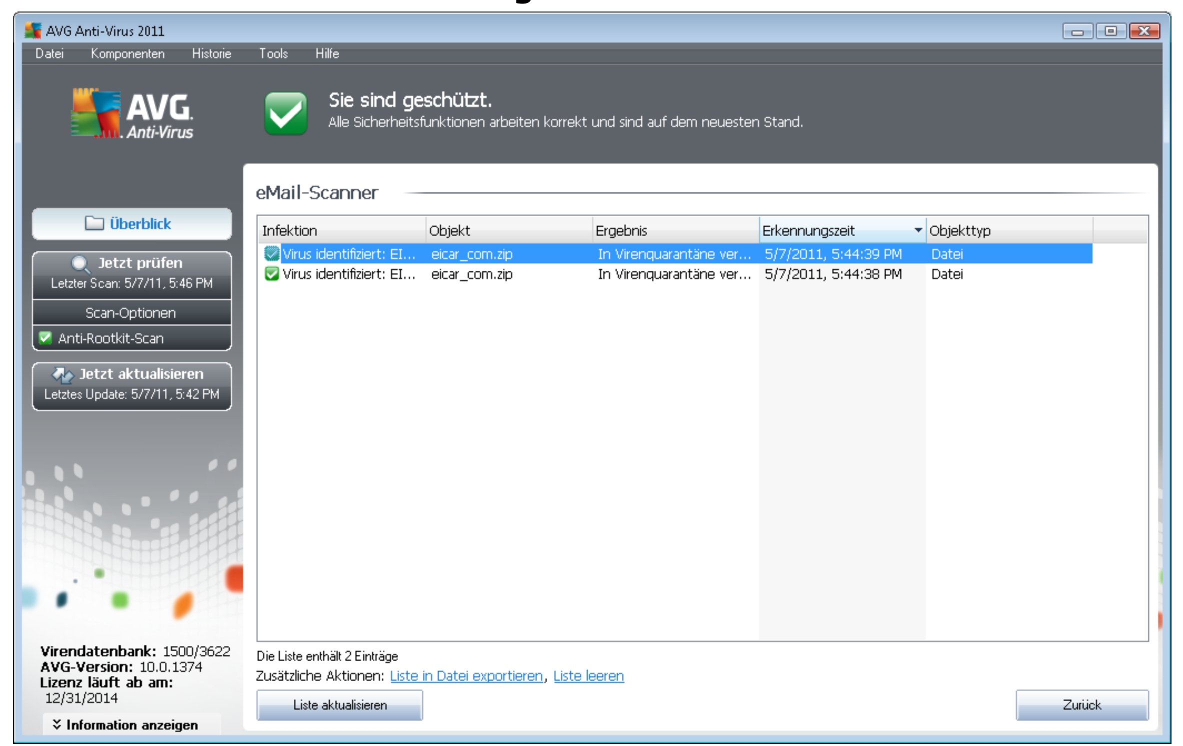
Auf der Benutzeroberfläche des ***eMail-Scanners*** sind folgende Schaltflächen verfügbar:

- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren



7.7.3. eMail-Scanner-Erkennung



Im Dialog ***eMail-Scanner-Erkennung*** *(erreichbar im Systemmenü über die Option „Historie/eMail-Scanner“*) wird eine Liste aller Funde angezeigt, die von der Komponente ***eMail-Scanner*** erkannt wurden. Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Infektion*** – Beschreibung (nach Möglichkeit auch Name) des erkannten Objekts
- ***Objekt*** - Speicherort des Objekts
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Der Zeitpunkt (Datum und Uhrzeit), zu dem das verdächtige Objekt entdeckt wurde
- ***Objekttyp*** - Typ des erkannten Objekts

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei exportieren***) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***).

Schaltflächen

Auf der Benutzeroberfläche der ***eMail-Scanner-Erkennung*** stehen die folgenden Schaltflächen zur Verfügung:



- ***Liste aktualisieren*** – Aktualisiert die Liste der erkannten Bedrohungen
- ***Zurück*** – Führt Sie zum zuvor angezeigten Dialog

7.8. Updatemanager

7.8.1. Grundlagen zum Updatemanager

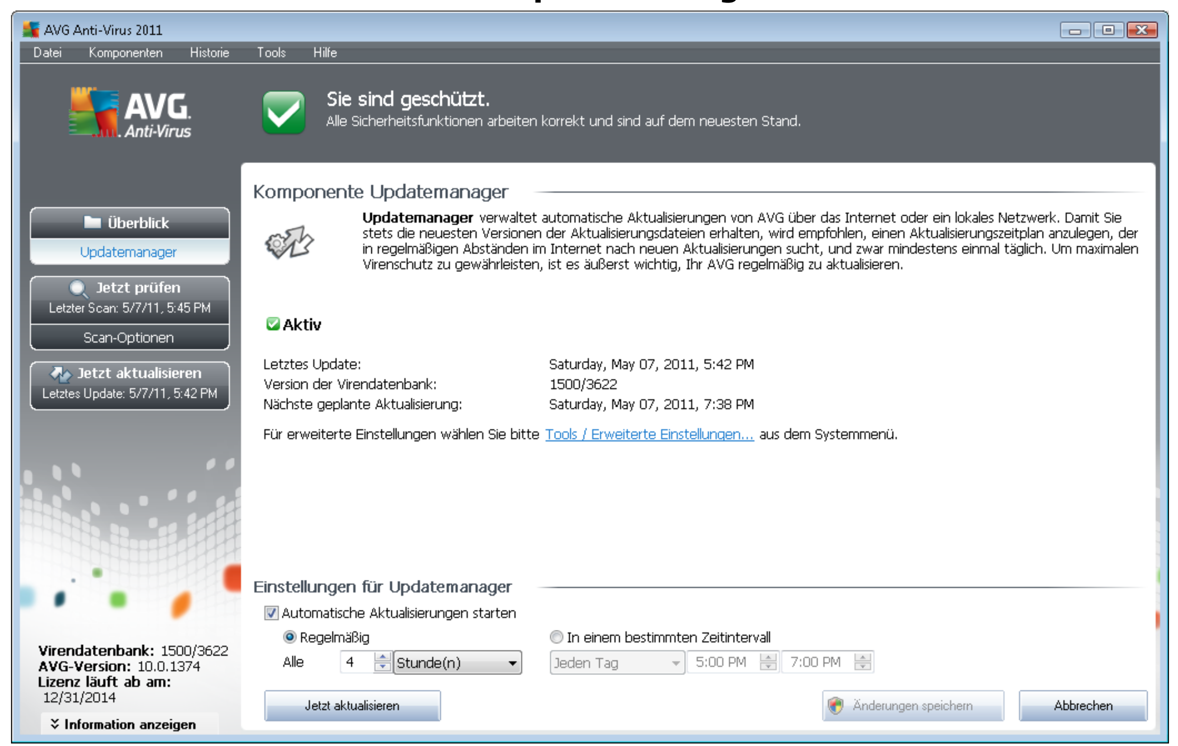
Keine Sicherheits-Software kann einen wirksamen Schutz gegen verschiedene Bedrohungen bieten, wenn sie nicht regelmäßig aktualisiert wird! Verfasser von Viren suchen stets nach neuen Lücken in Software und Betriebssystemen, die sie ausnutzen können. Jeden Tage gibt es neue Viren, neue Malware und neue Hacker-Angriffe. Software-Hersteller geben daher ständig neue Updates und Sicherheits-Patches heraus, mit denen entdeckte Sicherheitslücken geschlossen werden sollen.

Es ist entscheidend, dass Sie AVG regelmäßig aktualisieren!

Der ***Updatemanager*** hilft Ihnen dabei, regelmäßige Aktualisierungen zu steuern. In dieser Komponente können Sie das automatische Herunterladen von Aktualisierungsdateien aus dem Internet oder Ihrem lokalen Netzwerk planen. Wenn möglich, sollten Virendefinitionen täglich aktualisiert werden. Weniger dringende Programmupdates können wöchentlich gestartet werden.

Hinweis: *Im Kapitel AVG Updates finden Sie weitere Informationen zu Aktualisierungsstufen und -arten!*

7.8.2. Benutzeroberfläche des Updatemanagers





Die Oberfläche des ***Updatemanagers*** enthält Informationen zu den Funktionen der Komponente, ihren aktuellen Status und bietet wichtige statistische Daten:

- ***Letztes Update – Zeigt das Datum und die Zeit der letzten Datenbankaktualisierung an***
- ***Version der Virendatenbank*** – gibt die Versionsnummer der aktuell installierten Virendatenbank an; wird bei jedem Update der Virendatenbank erhöht
- ***Nächstes geplantes Update – Zeigt das Datum und die Zeit der nächsten Datenbankaktualisierung an***

Einstellungen für Update Manager

Im unteren Teil des Dialogs finden Sie den Bereich ***Einstellungen für Updatemanager***, in dem Sie einige Regeln des Aktualisierungsstarts ändern können. Sie können festlegen, ob die Aktualisierungsdateien automatisch (***Automatische Aktualisierungen starten***) oder On-Demand heruntergeladen werden sollen. Standardmäßig ist die Option ***Automatische Aktualisierungen starten*** aktiviert, und wir empfehlen, dies auch so zu belassen! Das regelmäßige Herunterladen der aktuellsten Updatedateien ist entscheidend für das Funktionieren jeder Sicherheits-Software!

Sie können weiter festlegen, wann das Update gestartet werden soll:

- o ***Regelmäßig*** – Hier können Sie das Zeitintervall festlegen
- o ***In einem bestimmten Zeitintervall*** – geben Sie die Startzeit für die Durchführung des Updates an

Standardmäßig ist das Update auf alle 4 Stunden eingestellt. Wenn Sie keinen wichtigen Grund haben, dies zu ändern, sollten Sie diese Einstellung beibehalten!

Hinweis: Alle *Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü den Eintrag* ***Tools / Erweiterte Einstellungen*** *aus, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

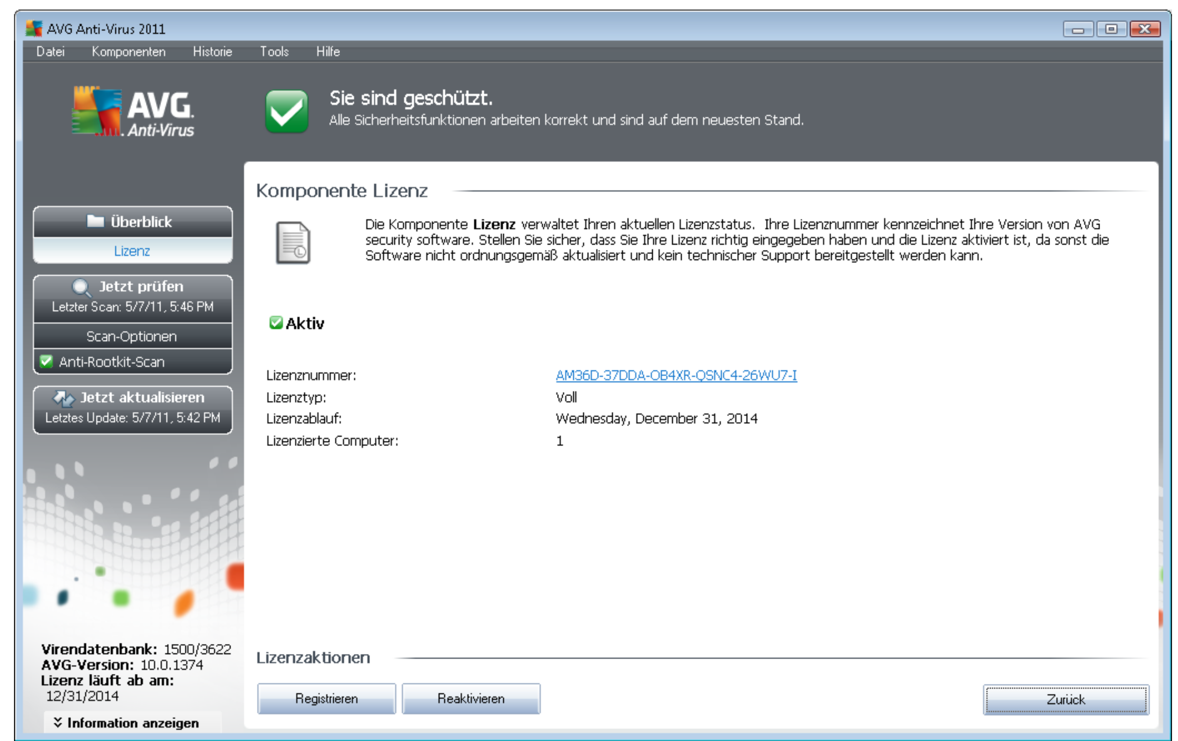
Schaltflächen

Auf der Oberfläche des ***Updatemanager*** stehen folgende Schaltflächen zur Verfügung:

- ***Jetzt aktualisieren*** – Hiermit wird das Update unmittelbar, On-Demand gestartet
- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren



7.9. Lizenz



Auf der Benutzeroberfläche der Komponente ***Lizenz*** finden Sie eine kurze Beschreibung der Funktionsweise der Komponente, Informationen zum aktuellen Status sowie die folgenden Informationen:

- ***Lizenznummer*** – bietet die verkürzte Form Ihrer Lizenznummer (*aus Sicherheitsgründen wurden die letzten vier Ziffern weggelassen*). Wenn Sie die Lizenznummer eingeben, müssen Sie diese absolut präzise und exakt wie angezeigt eingeben. Aus diesem Grund empfehlen wir ausdrücklich, zur Verwendung der Lizenznummer die Methode „Kopieren und Einfügen" zu nutzen.

- ***Lizenztyp*** – Gibt den installierten Produkttyp an.

- ***Lizenzablauf*** – Dieses Datum zeigt, wie lange Ihre Lizenz gültig ist. Wenn Sie **AVG Anti-Virus 2011** über dieses Datum hinaus weiter verwenden möchten, müssen Sie Ihre Lizenz verlängern. Die Verlängerung der Lizenz kann online auf der [Website von AVG](http://www.avg.com/de/) durchgeführt werden.

- ***Lizenzierte Computer*** – Gibt an, auf wie vielen Workstations **AVG Anti-Virus 2011** installiert werden darf.

Schaltflächen

- ***Registrieren*** – Stellt eine Verbindung zur Registrierungsseite der Website von AVG (http://www.avg.com/de/) her. Bitte geben Sie Ihre Registrierungsdaten ein; nur Kunden, die ihr AVG-Produkt registrieren, erhalten kostenlosen technischen Support.

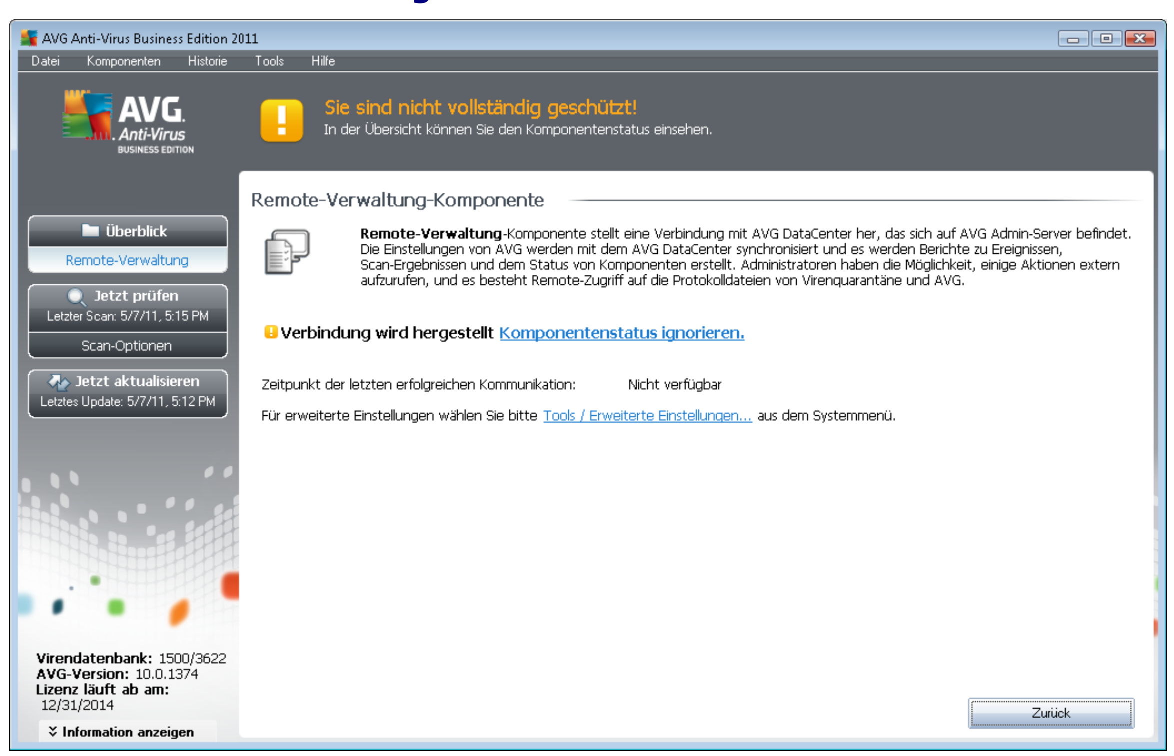


- ***Reaktivieren***– Öffnet den Dialog ***AVG aktivieren*** mit den Daten, die Sie im Dialog ***AVG personalisieren*** des Installationsvorgangs eingegeben haben. In diesem Dialog können Sie Ihre Lizenznummer eingeben, um entweder die Vertriebsnummer (*die Nummer, mit der Sie AVG installiert haben*) oder die alte Lizenznummer (*zum Beispiel beim Upgrade auf ein neues AVG-Produkt*) zu ersetzen.

Hinweis: *Wenn Sie die Testversion von* **AVG Anti-Virus 2011** *verwenden, werden die Schaltflächen als* ***Jetzt kaufen*** *und* ***Aktivieren*** *angezeigt und ermöglichen es Ihnen, die Vollversion des Programms zu erwerben. Wenn* **AVG Anti-Virus 2011** *mit einer Vertriebsnummer installiert ist, werden die Schaltflächen als* ***Registrieren*** *und* ***Aktivieren*** *angezeigt.*

- ***Zurück*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren.

7.10. Remote-Verwaltung



Die Komponente ***Remote-Verwaltung*** wird nur in der Benutzeroberfläche von **AVG Anti-Virus 2011** angezeigt, wenn Sie die Business Edition Ihres Produkts installiert haben (*siehe Komponente* ***Lizenz***). Im Dialog ***Remote-Verwaltung*** wird angezeigt, ob die Komponente aktiv und mit dem Server verbunden ist. Alle Einstellungen der Komponente ***Remote-Verwaltung*** werden in den ***Erweiterten Einstellungen/Remote-Verwaltung*** vorgenommen.

Eine genaue Beschreibung der Optionen und Funktionen der Komponente im System von AVG Remote-Verwaltung finden Sie in der Dokumentation speziell und ausschließlich zu diesem Thema. Diese Dokumentation kann von der AVG-Website (www.avg.de) unter ***Support Center > Download > Dokumentation*** heruntergeladen werden.



Schaltflächen

- ***Zurück*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückkehren.

7.11. Online Shield

7.11.1. Grundlagen zu Online Shield

Online Shield ist eine Art von Echtzeitschutz. Der Inhalt besuchter Webseiten (*und möglicher enthaltener Dateien*) wird gescannt, noch bevor diese Inhalte in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen werden.

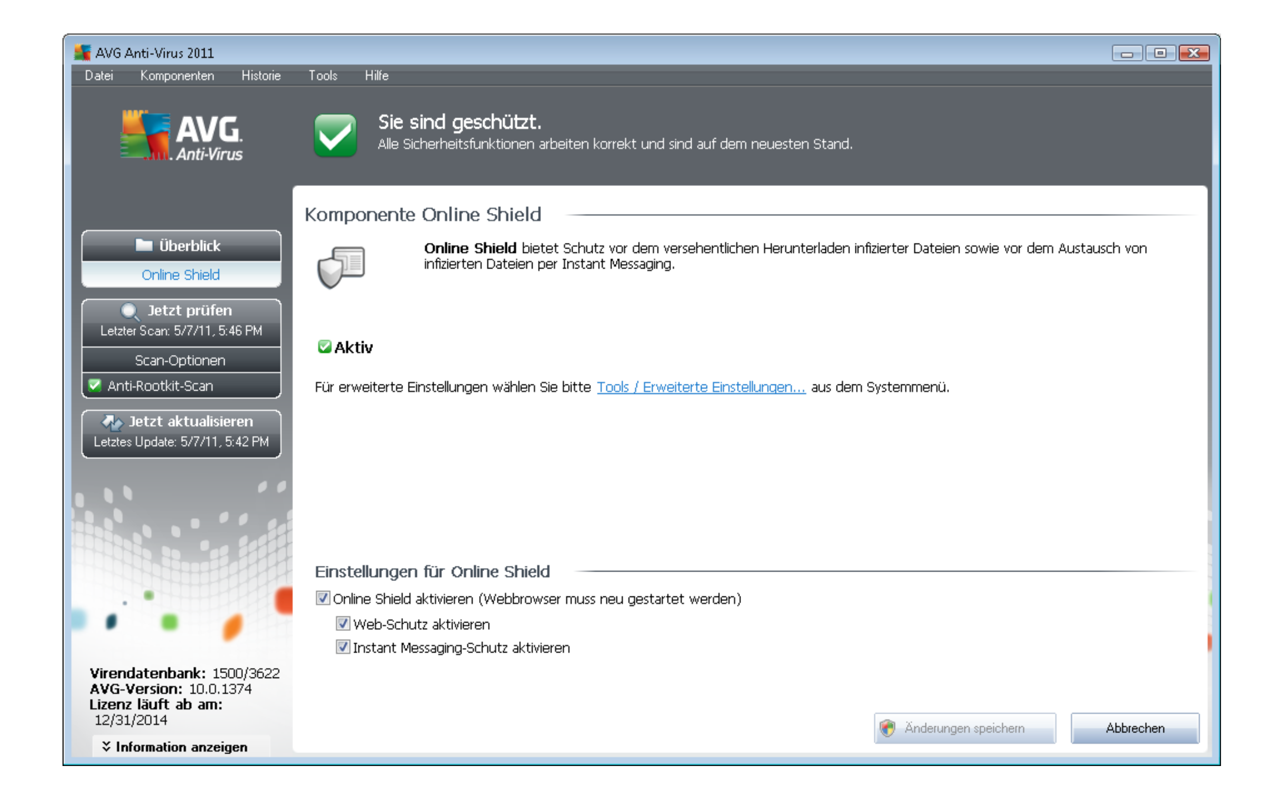
Online Shield erkennt, ob eine Seite, die Sie gerade besuchen, gefährliches Javascript enthält, und verhindert die Anzeige der Seite. Die Komponente erkennt auch die auf einer Seite enthaltene Malware, stoppt automatisch das Herunterladen und sorgt so dafür, dass sie niemals auf Ihren Computer gelangt.

Hinweis: *AVG Online Shield ist nicht für Serverplattformen vorgesehen!*

7.11.2. Benutzeroberfläche von Online Shield

Auf der Oberfläche der Komponente ***Online Shield*** wird das Verhalten dieses Schutzmechanismus beschrieben. Darüber hinaus finden Sie Informationen zum aktuellen Status der Komponente. Im unteren Bereich des Dialogs werden grundlegende Optionen zur Bearbeitung der Funktionsweise der Komponente angezeigt:





Einstellungen für Online Shield

Zunächst haben Sie die Möglichkeit, ***Online Shield*** jederzeit ein- und auszuschalten, indem Sie den Eintrag ***Online Shield aktivieren*** markieren. Standardmäßig ist die Option aktiviert, und die Komponente ***Online Shield*** ist aktiv. Es wird empfohlen, diese Einstellung beizubehalten, sofern Sie keinen wichtigen Grund haben, die Komponente zu deaktivieren. Wenn der Eintrag aktiviert ist und ***Online Shield*** ausgeführt wird, werden zwei weitere Optionen aktiviert:

- ***Web-Schutz aktivieren*** – Mit dieser Option wird bestätigt, dass ***Online Shield*** die Inhalte von Seiten im Internet scannen soll.

- ***Instant Messaging-Schutz aktivieren*** – Aktivieren Sie diese Option, um festzulegen, dass ***Online Shield*** Instant Messaging-Kommunikationen (*z. B. ICQ, MSN Messenger usw.*) auf Viren überprüfen soll.

Hinweis: Alle *Komponenten von AVG sind vom Hersteller standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden. Wenn Sie Änderungen an der Konfiguration von AVG vornehmen müssen, wählen Sie im Menü den Eintrag* ***Tools / Erweiterte Einstellungen*** *aus, und bearbeiten Sie die Konfiguration von AVG im angezeigten Dialog Erweiterte AVG-Einstellungen.*

Schaltflächen

Auf der Oberfläche von ***Online Shield*** stehen folgende Schaltflächen zur Verfügung:



- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zum Hauptfenster der ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren

7.11.3. Erkennung durch Online Shield

Online Shield scannt den Inhalt besuchter Webseiten und möglicher enthaltener Dateien, noch bevor dieser in Ihrem Webbrowser angezeigt oder auf Ihren Computer heruntergeladen wird. Wenn eine Bedrohung erkannt wird, werden Sie unmittelbar mit folgendem Dialog gewarnt:



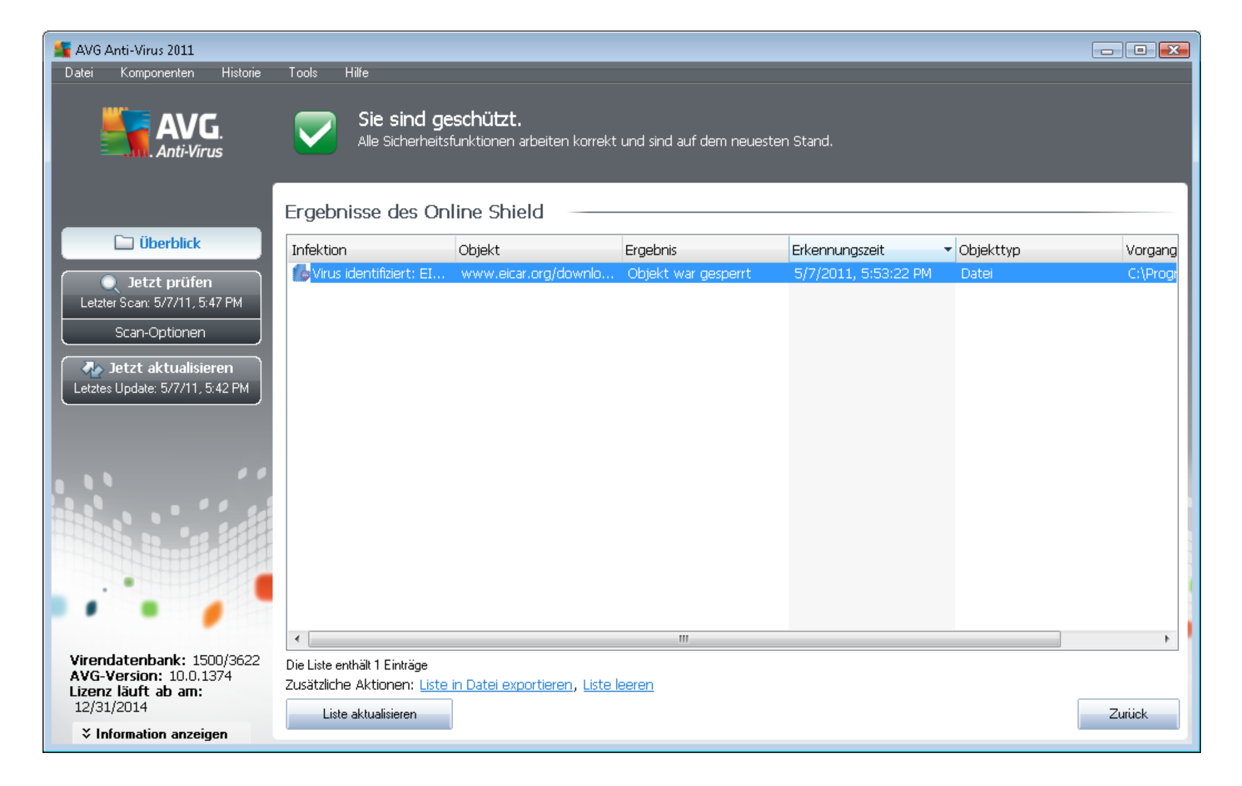
In diesem Warndialog finden Sie Informationen zu der Datei, die als infiziert erkannt wurde (*Dateiname*), den Namen der erkannten Bedrohung (*Name der Bedrohung*) und einen Link zur ***Virenenzyklopädie***, wo Sie weitere Informationen zur erkannten Infektion finden (*falls bekannt*). Der Dialog enthält folgende Schaltflächen:

- ***Details anzeigen*** – Klicken Sie auf ***Details anzeigen***, um ein Popup-Fenster mit der Prozesskennung und weiteren Informationen zum Prozess anzuzeigen, der beim Erkennen der Infektion ausgeführt wurde.

- ***Schließen*** – Klicken Sie auf diese Schaltfläche, um den Warndialog zu schließen.

Die verdächtige Webseite wird nicht geöffnet, und die erkannte Bedrohung wird in die Liste der ***Funde von Online Shield*** eingetragen – Diese Übersicht der entdeckten Bedrohungen können Sie im Systemmenü unter ***Verlauf/Funde von Online Shield*** aufrufen.





Zu jedem erkannten Objekt werden folgende Informationen angegeben:

- ***Infektion*** – Beschreibung (*nach Möglichkeit auch Name*) des erkannten Objekts
- ***Objekt*** – Quelle des Objekts (*Webseite*)
- ***Ergebnis*** - Aktion, die mit dem erkannten Objekt ausgeführt wurde
- ***Erkennungszeit*** – Zeitpunkt (Datum und Uhrzeit), zu dem die Bedrohung entdeckt und blockiert wurde
- ***Objekttyp*** - Typ des erkannten Objekts
- ***Vorgang*** - Ausgeführte Aktion, mit der das potentiell gefährliche Objekt aufgerufen wurde, so dass es erkannt werden konnte

Im unteren Bereich des Dialogs – unter der Liste – finden Sie Informationen zur Gesamtanzahl der erkannten Objekte, die im oberen Bereich aufgelistet sind. Sie können die gesamte Liste erkannter Objekte in eine Datei exportieren (***Liste in Datei exportieren***) und alle Einträge zu erkannten Objekten löschen (***Liste leeren***). Die Schaltfläche ***Liste aktualisieren*** aktualisiert die Liste der von ***Online Shield*** erkannten Funde. Mit der Schaltfläche ***Zurück*** können Sie zurHauptseite der ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren.



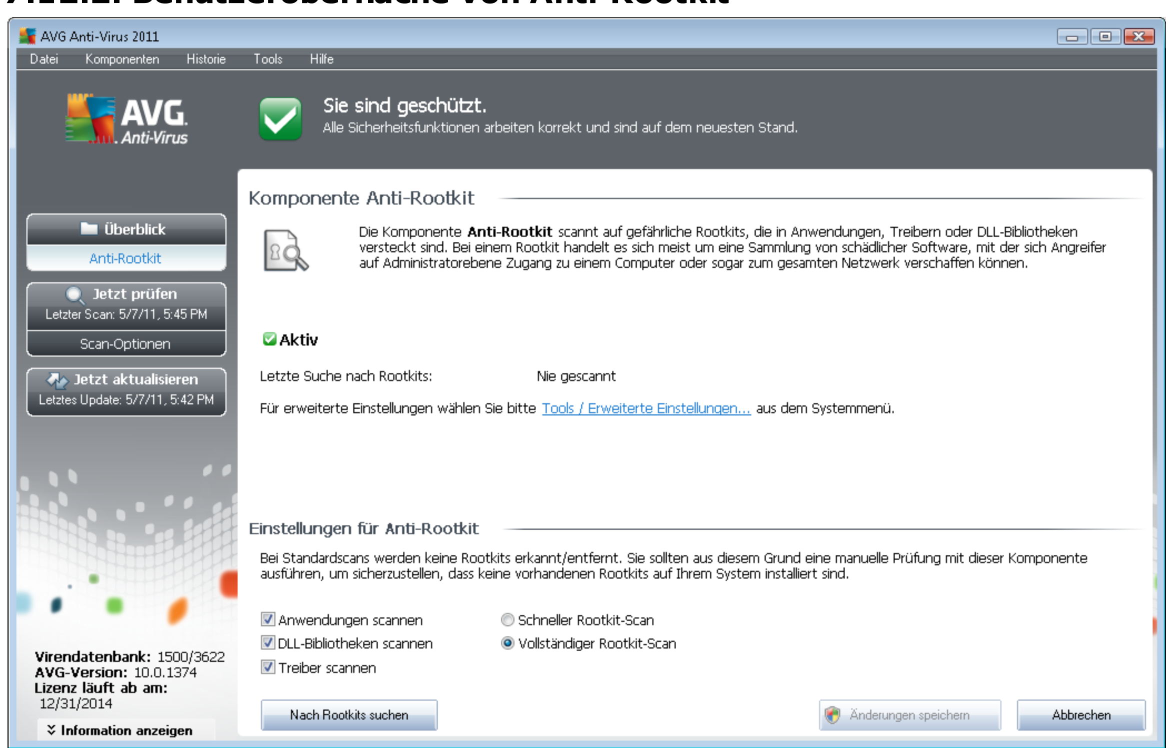
7.12. Anti-Rootkit

Ein Rootkit ist ein Programm, das ohne Genehmigung der Systembesitzer oder berechtigten Manager die Kontrolle über ein Computersystem übernimmt. Ein Zugriff auf die Hardware ist meist nicht erforderlich, da ein Rootkit darauf abzielt, die Kontrolle über das Betriebssystem, das auf der Hardware ausgeführt wird, zu übernehmen. Rootkits verbergen ihre Existenz auf dem System üblicherweise, indem sie die standardmäßigen Sicherheitsmechanismen des Betriebssystems außer Kraft setzen oder umgehen. Oft handelt es sich bei diesen Programmen gleichzeitig um Trojaner, die bei Benutzern den Eindruck erwecken, sie könnten ohne Risiko auf ihren Systemen ausgeführt werden. Dies wird mit Techniken wie dem Verbergen von ausgeführten Prozessen vor Überwachungsprogrammen oder dem Verbergen von Dateien oder Systemdaten vor dem Betriebssystem erzielt.

7.12.1. Grundlagen zu Anti-Rootkit

AVG Anti-Rootkit ist ein spezielles Tool für die Erkennung und wirksame Entfernung gefährlicher Rootkits, also von Programmen und Technologien, die die Anwesenheit schädlicher Software auf Ihrem Computer verbergen können. ***AVG Anti-Rootkit*** erkennt Rootkits auf Basis eines vordefinierten Regelsatzes. Bitte beachten Sie, dass alle Rootkits erkannt werden (*nicht nur die infizierten*). Wenn ***AVG Anti-Rootkit*** ein Rootkit entdeckt, heißt das nicht unbedingt, dass das Rootkit auch infiziert ist. Manchmal werden Rootkits als Treiber eingesetzt oder sie gehören zu ordnungsgemäßen Anwendungen.

7.12.2. Benutzeroberfläche von Anti-Rootkit



Die Benutzeroberfläche von ***Anti-Rootkit*** enthält eine kurze Beschreibung der Funktionen der Komponente, gibt Auskunft über den Status der Komponente und enthält Informationen über den



Zeitpunkt des letzten mit ***Anti-Rootkit*** (***Letzte Suche nach Rootkits***) durchgeführten Tests. Der Dialog ***Anti-Rootkit*** enthält außerdem den Link ***Tools/Erweiterte Einstellungen***. Klicken Sie auf diesen Link, um erweiterte Konfigurationen für die Komponente ***Anti-Rootkit*** vorzunehmen.

Hinweis:*Alle Komponenten von AVG sind standardmäßig so eingestellt, dass eine optimale Leistung erzielt wird. Ändern Sie die Konfiguration von AVG nur, wenn Sie einen besonderen Grund dazu haben. Änderungen an den Einstellungen sollten nur von erfahrenen Benutzern durchgeführt werden.*

Einstellungen für Anti-Rootkit

Im unteren Teil des Dialogs finden Sie den Bereich ***Einstellungen für Anti-Rootkit***, in dem Sie einige grundlegende Funktionen für das Scannen nach vorhandenen Rootkits einstellen können. Markieren Sie zunächst die entsprechenden Kontrollkästchen, um festzulegen, welche Objekte gescannt werden sollen:

- ***Anwendungen scannen***
- ***DLL-Bibliotheken scannen***
- ***Treiber scannen***

Wählen Sie anschließend den Rootkit-Scanmodus aus:

- ***Schneller Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber und den Systemordner (*typischerweise C:\WINDOWS*)
- ***Vollständiger Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber, den Systemordner (*typischerweise C:\WINDOWS*) und zusätzlich alle lokalen Festplatten (*einschließlich Flash-Disks, aber keine Disketten-/CD-Laufwerke*)

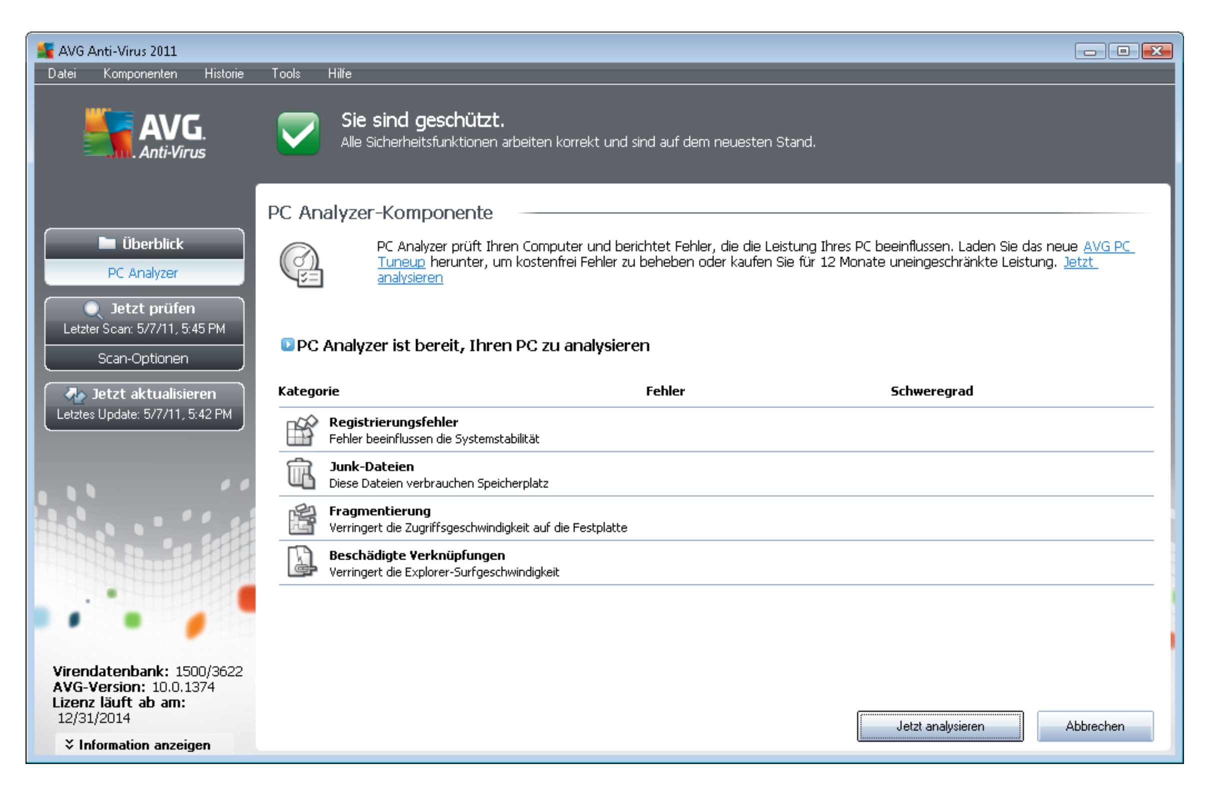
Schaltflächen

- ***Nach Rootkits suchen*** – Da der Rootkit-Scan kein integrierter Bestandteil des ***Scans für den gesamten Computer*** ist, können Sie den Rootkit-Scan mit dieser Schaltfläche direkt über die Benutzeroberfläche von ***Anti-Rootkit*** ausführen
- ***Änderungen speichern*** – Mit dieser Schaltfläche können Sie alle auf dieser Benutzeroberfläche vorgenommenen Änderungen speichern und zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren
- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren, ohne Ihre Änderungen zu speichern



7.13. PC Analyzer

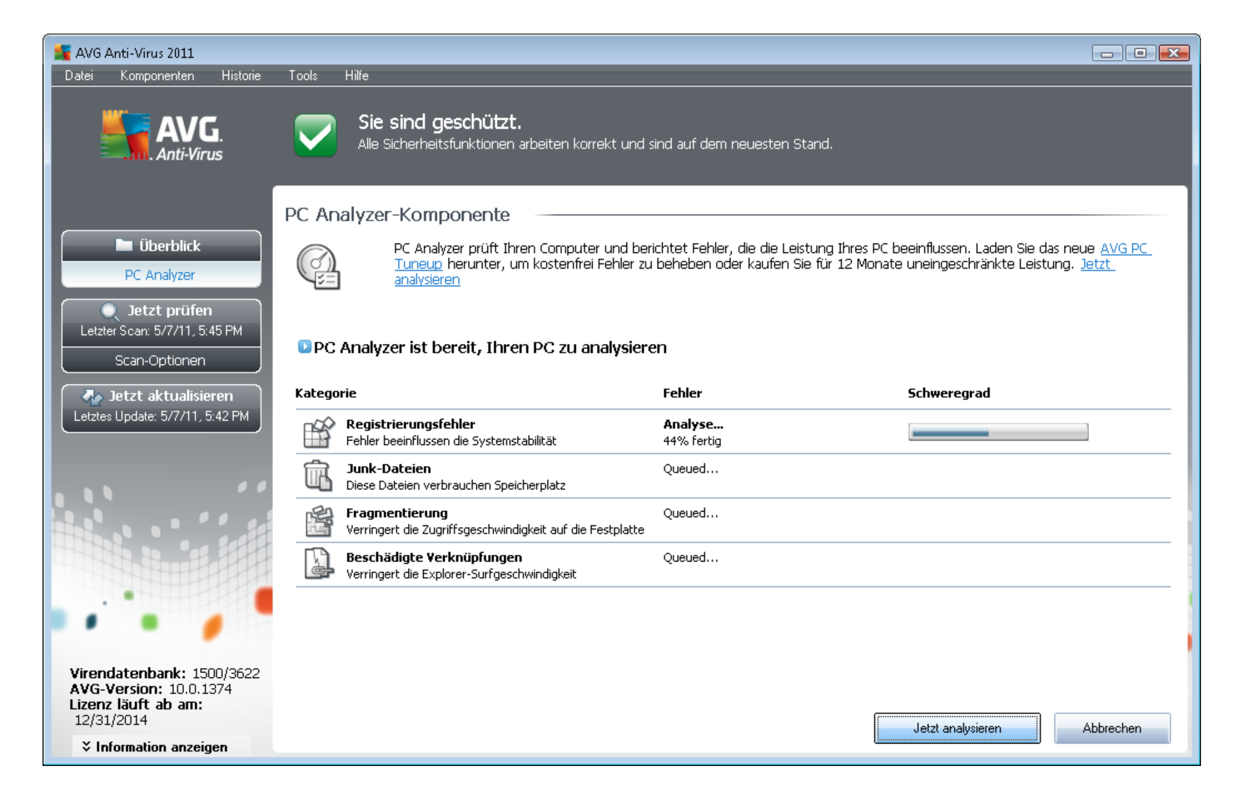
Die Komponente ***PC Analyzer*** überprüft Ihren Computer auf Systemprobleme und zeigt anschließend in einer Übersicht mögliche Gründe für die beeinträchtigte Leistung Ihres Computers an. Auf der Benutzeroberfläche der Komponente wird ein Diagramm angezeigt, das in die folgenden vier Kategorien eingeteilt ist: Registrierungsfehler, Junk-Dateien, Fragmentierung und beschädigte Verknüpfungen:



- ***Registrierungsfehler***: Gibt die Anzahl der Fehler in der Windows-Registrierung an. Da die Fehlerbehebung der Registrierung spezifische Kenntnisse erfordert, wird die selbständige Reparatur der Registrierung nicht empfohlen.
- ***Junk-Dateien***: Gibt die Anzahl der Dateien an, die mit großer Wahrscheinlichkeit nicht benötigt werden. Dazu gehören typischerweise temporäre Dateien und Dateien, die sich im Papierkorb befinden.
- ***Fragmentierung***: Berechnet die Fragmentierung Ihrer Festplatte in Prozent. Mit Fragmentierung bezeichnet man die Speicherung von Datenbeständen, die nach einem langen Zeitraum über die gesamte Festplatte verteilt sind. Sie können dieses Problems mit einem Defragmentierungs-Tool beheben.
- ***Beschädigte Verknüpfungen***: Benachrichtigt Sie über Verknüpfungen, die nicht mehr funktionieren oder auf nicht vorhandene Speicherorte verweisen usw.

Klicken Sie auf ***Jetzt analysieren***, um eine Analyse Ihres Systems zu starten. Sie können den Analysefortschritt nachvollziehen und die Ergebnisse der Analyse direkt im Diagramm sehen:





In der Ergebnisübersicht werden die erkannten Systemprobleme (***Fehler***) in den entsprechenden, überprüften Kategorien aufgelistet. Die Ergebnisse der Analyse werden außerdem grafisch auf einer Achse in der Spalte ***Schweregrad*** angeordnet.

Schaltflächen

- ***Jetzt analysieren*** (*wird vor dem Start der Analyse angezeigt*) – Klicken Sie auf diese Schaltfläche, um eine sofortige Analyse Ihres Computer zu starten
- ***Fehler jetzt beheben*** (*wird nach Abschluss der Analyse angezeigt*) – Klicken Sie auf diese Schaltfläche, um eine Seite der Website von AVG (http://www.avg.com/de/) aufzurufen, auf der Sie genaue und aktuelle Informationen zur Komponente ***PC Analyzer*** erhalten
- ***Abbrechen*** – Klicken Sie auf diese Schaltfläche, um die Analyse abzubrechen oder um nach Abschluss der Analyse zur Benutzeroberfläche von AVG (*Komponentenübersicht*) zurückzukehren

7.14. Identitätsschutz

AVG Identitätsschutz ist ein Anti-Malware-Produkt, das Identitätsdiebe daran hindert, Ihre Kennwörter, Bankkontodetails, Kreditkartennummern und andere persönliche Daten zu stehlen, wozu sie verschiedene Arten bösartiger Software (*Malware*) verwenden, die es auf Ihren Computer absehen. Es sorgt sicher, dass alle auf Ihrem Computer ausgeführten Programme ordnungsgemäß funktionieren. ***AVG Identitätsschutz*** erkennt und blockiert kontinuierlich verdächtiges Verhalten und schützt Ihren Computer vor neuer Malware.

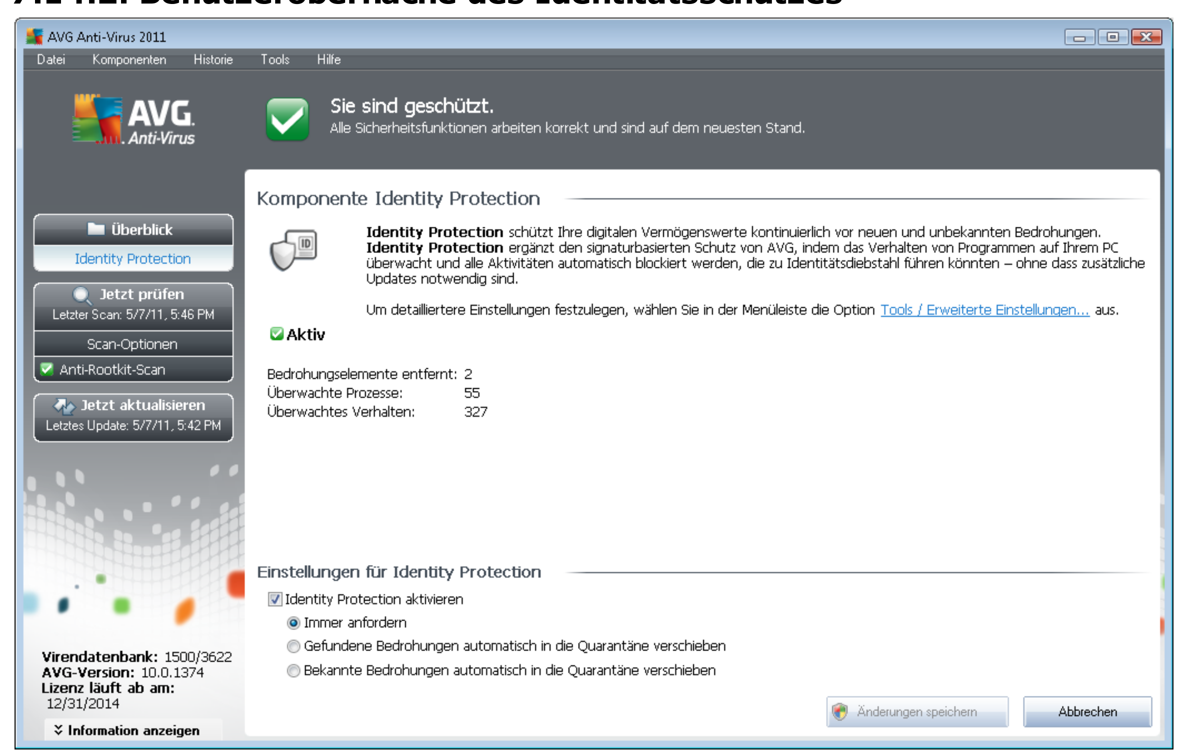


7.14.1. Grundlagen des Identitätsschutzes

AVG Identitätsschutz ist eine Anti-Malware-Komponente, die Sie mithilfe von Verhaltenstechnologien vor allen Arten von Malware schützt(*Spyware, Bots, Identitätsdiebstahl usw.*) und mit dem Zero-Day-Schutz vor neuen Viren bewahrt. Während Malware immer komplexer wird und in Form normaler Programme auftreten kann, mit denen Identitätsräuber in Ihren Computer eindringen, schützt Sie ***AVG Identitätsschutz*** vor dieser Art ausführungsbasierter Malware. Es handelt sich um einen Zusatzschutz für ***AVG Anti-Virus***, der Sie auf Grundlage von Signatur- und Scanverfahren vor dateibasierten und bekannten Viren schützt.

Wir empfehlen Ihnen dringend, sowohl AVG Anti-Virus als auch AVG Identitätsschutz zu installieren, um einen vollständigen Schutz Ihres PCs zu gewährleisten.

7.14.2. Benutzeroberfläche des Identitätsschutzes



Die Benutzeroberfläche der Komponente ***Identitätsschutz*** umfasst eine kurze Beschreibung der Grundfunktionen der Komponente, ihren Status sowie einige statistische Daten:

- ***Entfernte Malware-Elemente*** – Gibt die Zahl der als Malware ermittelten und entfernten Anwendungen an
- ***Überwachte Prozesse*** – Die Zahl der momentan ausgeführten Anwendungen, die mit dem Identitätsschutz überwacht werden
- ***Überwachtes Verhalten*** – Die Zahl der spezifischen Aktionen, die in den überwachten Anwendungen ausgeführt werden



Einstellungen für Identity Protection

Im unteren Bereich des Dialogs finden Sie die ***Einstellungen für Identitätsschutz***, wo Sie bestimmte Grundfunktionen der Komponente bearbeiten können:

- ***Identitätsschutz aktivieren*** – (*standardmäßig aktiviert*): Aktivieren Sie diese Option, um den Identitätsschutz zu aktivieren und weitere Bearbeitungsoptionen zu öffnen.

  In manchen Fällen meldet ***Identitätsschutz***, dass eine seriöse Datei verdächtig oder gefährlich ist. Da ***Identitätsschutz*** Bedrohungen auf Grundlage ihres Verhaltens erkennt, tritt dies normalerweise dann auf, wenn ein Programm versucht, gedrückte Tasten zu überwachen, andere Programme oder einen neuen Treiber auf dem Computer zu installieren. Wählen Sie daher bitte eine der folgenden Optionen, um das Verhalten von ***Identitätsschutz*** bei Erkennung einer verdächtigen Aktivität festzulegen:

  - ***Immer anfordern*** – Wenn eine Anwendung als Malware erkannt wird, werden Sie gefragt, ob diese blockiert werden soll (*diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Einstellung nur dann zu ändern, wenn Sie einen guten Grund dafür haben*)

  - ***Gefundene Bedrohungen automatisch in die Quarantäne verschieben*** – Alle als Malware erkannten Anwendungen werden automatisch blockiert

  - ***Bekannte Bedrohungen automatisch in die Quarantäne verschieben*** – Nur Anwendungen, bei denen es sich mit absoluter Sicherheit um Malware handelt, werden blockiert

Schaltflächen

Auf der Benutzeroberfläche von ***Identitätsschutz*** stehen folgende Schaltflächen zur Verfügung:

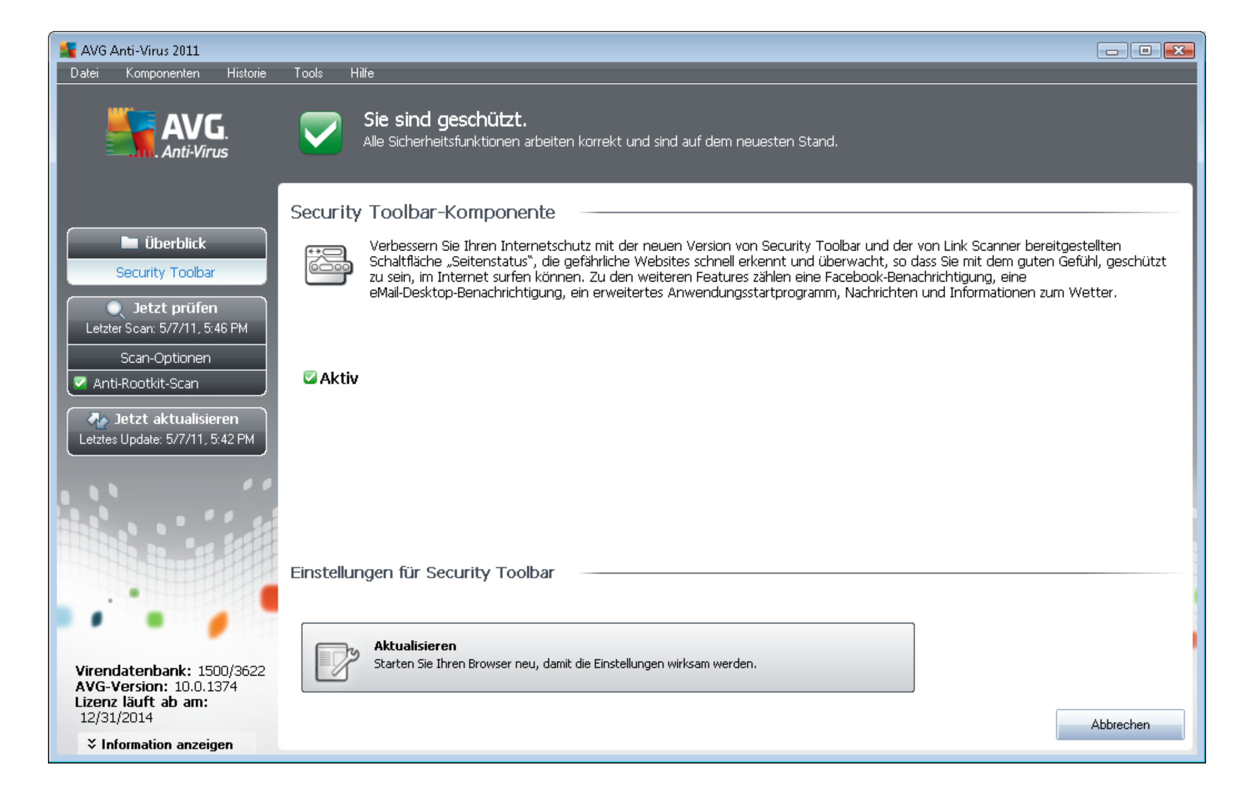
- ***Änderungen speichern*** – Klicken Sie auf diese Schaltfläche, um die in diesem Dialog vorgenommenen Änderungen zu speichern und zu übernehmen

- ***Abbrechen*** – Mit dieser Schaltfläche können Sie zur ***Benutzeroberfläche von AVG*** (*Komponentenübersicht*) zurückkehren

7.15. Security Toolbar

Die ***Security Toolbar*** ist eine optionale Webbrowser-Symbolleiste, die erweiterten AVG-Schutz sowie verschiedene nützliche Funktionen und Tools beim Surfen im Internet bietet. Derzeit wird die ***Security Toolbar*** von den Webbrowsern Internet Explorer (*6.0 oder höher)* und Mozilla Firefox *(3.0 oder höher*) unterstützt:





Auf alle Einstellungen der Komponente ***Security Toolbar*** kann direkt in der ***Security Toolbar*** in Ihrem Webbrowser zugegriffen werden.



8. AVG Security Toolbar installieren

AVG Security Toolbar ist ein neues Tool, das mit dem [***LinkScanner***]() ***zusammenarbeitet.*** Die ***AVG Security Toolbar*** kann zur Steuerung der Funktionen von [***Link Scanner***]() und zum Anpassen des Verhaltens dieser Komponente verwendet werden.

Wenn Sie bei der Installation von **AVG Anti-Virus 2011** die Toolbar ebenfalls installieren, wird diese Ihrem Webbrowser (*Internet Explorer 6.0 oder höher, Mozilla Firefox 3.0 oder höher*) automatisch hinzugefügt. Andere Internetbrowser werden derzeit nicht unterstützt.

Hinweis: *Wenn Sie einen alternativen Browser verwenden (zum Beispiel Avant), kann unerwartetes Verhalten auftreten.*

8.1. Benutzeroberfläche der AVG Security Toolbar

Die ***AVG Security Toolbar*** ist für die Arbeit mit ***MS Internet Explorer*** (*Version 6.0 oder höher*) und ***Mozilla Firefox*** (*Version 3.0 oder höher*) ausgelegt. Nachdem Sie sich entschieden haben, die ***AVG Security Toolbar*** zu installieren (*während der [Installation von AVG]() wurden Sie gefragt, ob Sie die Komponente installieren möchten oder nicht*), wird die Komponente in Ihrem Webbrowser unterhalb der Adresszeile angezeigt:



Die ***AVG Security Toolbar*** enthält die folgenden Elemente:

8.1.1. Schaltfläche mit dem AVG-Logo

Diese Schaltfläche bietet Zugang zu allgemeinen Funktionen der Symbolleiste. Wenn Sie auf die Schaltfläche mit dem Logo klicken, werden Sie auf die [Website von AVG]() weitergeleitet. Wenn Sie neben das AVG-Symbol klicken, wird eines der folgenden Elemente geöffnet:

- ***Toolbar Info*** – Link zur Homepage der ***AVG Security Toolbar mit ausführlichen Informationen, wie die Toolbar zu Ihrem Schutz beiträgt.***
- ***AVG starten*** – Öffnet die **AVG Anti-Virus 2011** [***Benutzeroberfläche von AVG***]()
- ***AVG Info*** – Öffnet ein Kontextmenü mit Links, die zu sicherheitsrelevanten Informationen zu **AVG Anti-Virus 2011** führen:
    - o *Infos zu Bedrohungen* – Öffnet die [Website von AVG]() und führt sie zu einer Seite mit wichtigen Informationen zu Bedrohungen, Empfehlungen zum Entfernen von Viren, Informationen zu AVG-Updates, Zugriff auf die [Virendatenbank]() und weiteren wichtigen Informationen
    - o *AVG Neuigkeiten* – Öffnet die Webseite mit den neuesten Pressemitteilungen über AVG



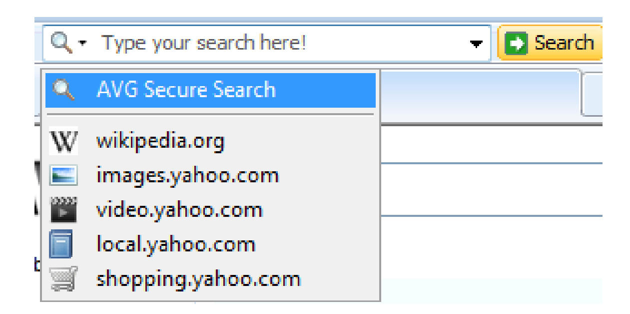
  - o *Aktuelle Bedrohungsstufe* – Öffnet die Webseite des Virenlabors mit einer grafischen Darstellung der aktuellen Bedrohungslage im Internet
  - o *AVG Threat Labs* – Öffnet die Website AVG SiteReports, auf der Sie Bedrohungen nach Namen suchen können und weitere Informationen zu den einzelnen Bedrohungen erhalten

- ***Optionen*** – Öffnet einen Konfigurationsdialog, in dem Sie die Einstellungen der ***AVG Security Toolbar*** an Ihre Anforderungen anpassen können – siehe folgendes Kapitel ***Optionen der AVG Security Toolbar***
- ***Verlauf löschen*** – Mit dieser Option können Sie über die ***AVG Security Toolbar*** den gesamten Verlauf löschen oder den Suchverlauf, Browserverlauf, Download-Verlauf oder Cookies einzeln löschen.
- ***Aktualisieren*** – überprüft, ob neue Updates für Ihre ***AVG Security Toolbar vorhanden sind***
- ***Hilfe*** – bietet Optionen zum Öffnen der Hilfedatei, zum Kontaktieren des technischen Supports von AVG, zum Senden von Produkt-Feedback oder zum Anzeigen der aktuellen Version der Toolbar

8.1.2. AVG Secure Search (powered by Google)-Suchfeld

Das***AVG Secure Search (powered by Google)***-Suchfeld bietet einen bequemen und sicheren Weg, um das Internet mit der Suchmaschine von AVG Secure Search (powered by Google) zu durchsuchen. Geben Sie ein Wort oder eine Wortgruppe in das Suchfeld ein und klicken Sie auf ***Suchen*** oder die ***Eingabetaste***, um die Suche direkt auf dem AVG Secure Search (powered by Google)-Server auszuführen, unabhängig davon, welche Seite derzeit angezeigt wird. Im Suchfeld wird auch Ihr Suchverlauf angezeigt. Suchen, die Sie über das Suchfeld durchführen, werden mit ***Search-Shield*** geprüft.

Alternativ können Sie im Suchfeld auch zu Wikipedia oder einer anderen Suchmaschine wechseln – siehe Abbildung:



8.1.3. Seitenstatus

Diese Schaltfläche zeigt anhand von Kriterien der Komponente ***Surf-Shield*** eine Bewertung der aktuell geladenen Webseite direkt in der Toolbar an:

- – Die verlinkte Seite stellt kein Sicherheitsrisiko dar

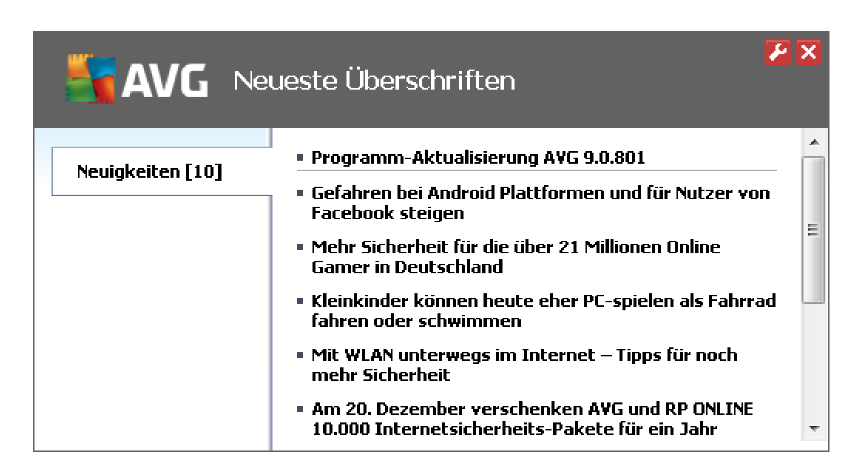


- – Die Seite ist leicht verdächtig.
- – Die Seite umfasst Links zu eindeutig gefährlichen Seiten.
- – Die verlinkte Seite enthält aktive Bedrohungen! Aus Sicherheitsgründen können Sie nicht auf diese Seite zugreifen.
- – Die Seite konnte nicht gescannt werden, da der Zugriff nicht möglich ist.

Klicken Sie auf diese Schaltfläche, um einen Informationsbereich mit genaueren Daten zu der bestimmten Webseite anzuzeigen.

8.1.4. AVG Neuigkeiten

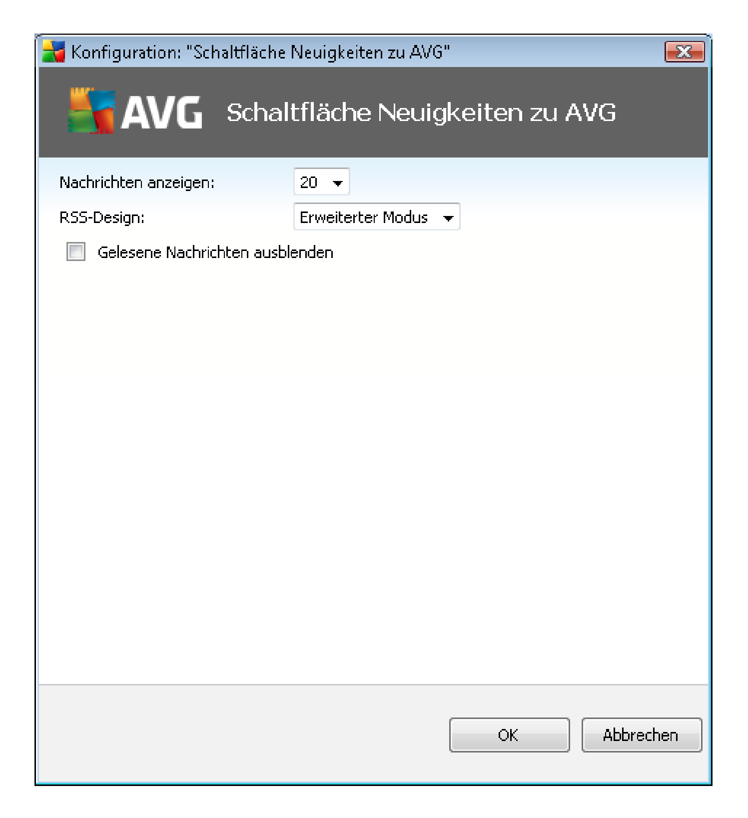
Mit dieser Schaltfläche in der ***AVG Security Toolbar*** können Sie eine Übersicht über die aktuellsten ***Schlagzeilen*** zu AVG aus der Presse und aus Pressemitteilungen des Unternehmens anzeigen:



In der oberen rechten Ecke werden zwei rote Schaltflächen angezeigt:

- – Durch Klicken auf diese Schaltfläche wird der Bearbeitungsdialog angezeigt, in dem Sie die Parameter für die Schaltfläche ***AVG Neuigkeiten*** in der ***AVG Security Toolbar*** festlegen können:





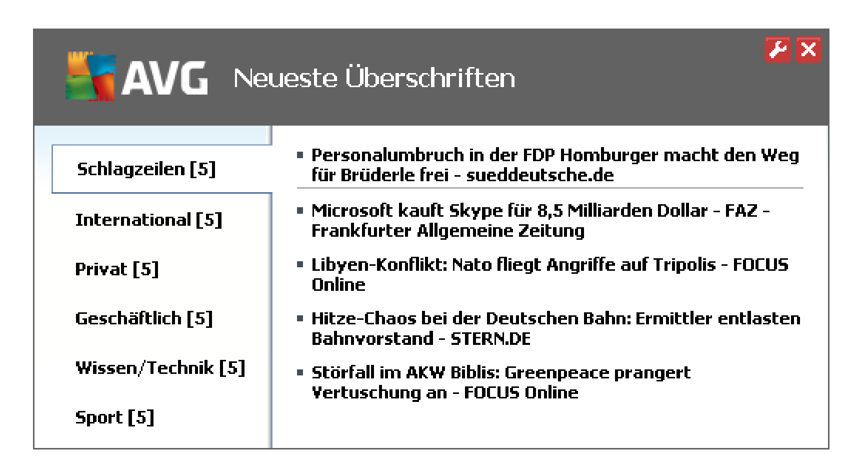
- o ***Nachrichten anzeigen*** – Legen Sie hier fest, wie viele Nachrichten gleichzeitig angezeigt werden sollen
- o ***RSS-Design*** – Wählen Sie hier den Anzeigemodus (Erweitert oder Standard) für die Übersicht über Neuigkeiten aus (*standardmäßig ist der Modus „Erweitert" ausgewählt – sie Abbildung oben*)
- o ***Gelesene Nachrichten ausblenden*** – Aktivieren Sie diesen Eintrag, um gelesene Nachrichten nicht mehr anzuzeigen, so dass neue Nachrichten nachrücken können

- ☒ – Klicken Sie auf diese Schaltfläche, um die Übersicht über Neuigkeiten zu schließen



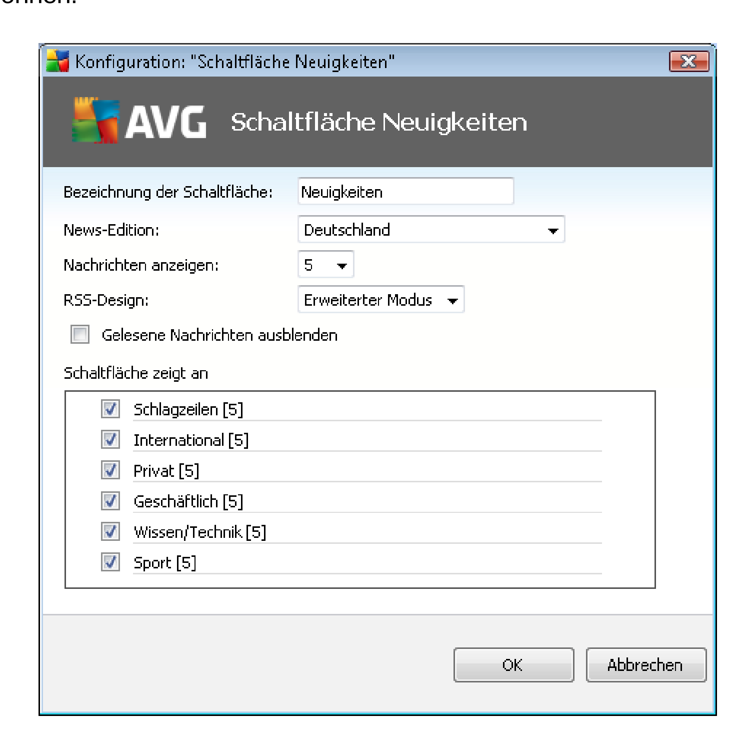
8.1.5. News

Direkt über die ***AVG Security Toolbar*** wird über diese Schaltfläche eine Übersicht über Neuigkeiten von ausgewählten Medien angezeigt und in verschiedene Bereiche eingeteilt:



In der oberen rechten Ecke werden zwei rote Schaltflächen angezeigt:

- – Durch Klicken auf diese Schaltfläche wird der Bearbeitungsdialog angezeigt, in dem Sie die Parameter für die Schaltfläche ***Neuigkeiten*** in der ***AVG Security Toolbar*** festlegen können:



o ***Bezeichnung der Schaltfläche*** – Sie können den Namen der Schaltfläche ändern, wie er in ***AVG Security Toolbar angezeigt wird***

o ***News-Edition*** – Wählen Sie ein Land aus der Liste aus, um Neuigkeiten aus dieser Region anzuzeigen



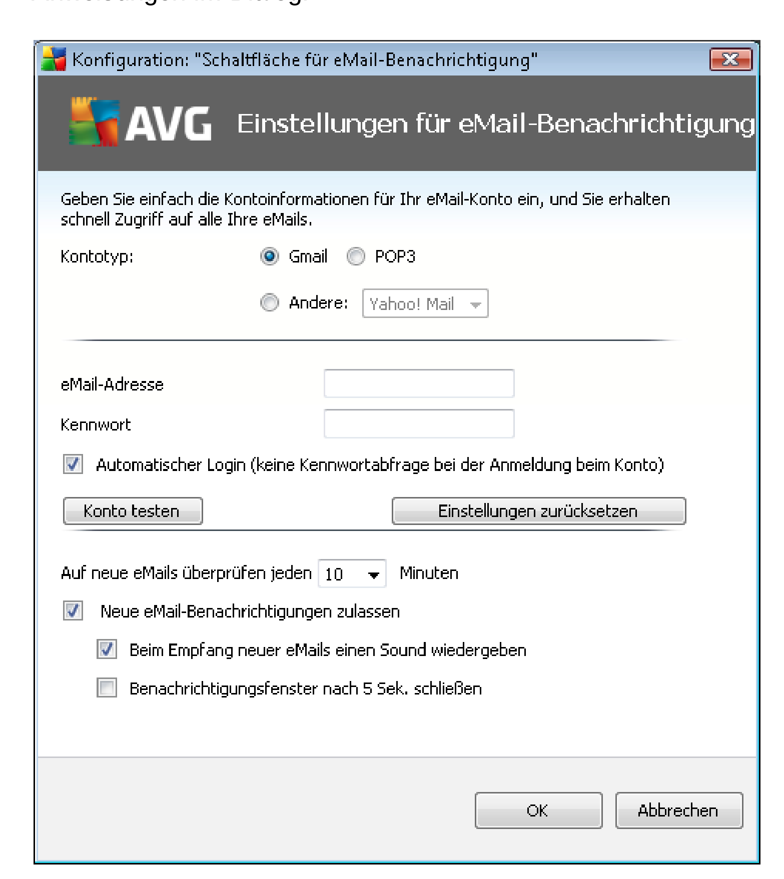
- o ***Nachrichten anzeigen*** – Legen Sie hier fest, wie viele Nachrichten gleichzeitig angezeigt werden sollen
- o ***RSS-Design*** – Wählen Sie hier die Option „Basis/Erweitert“ für die Anzeige der Übersicht über Neuigkeiten aus (***standardmäßig ist der Modus „Erweitert“ ausgewählt, siehe Abbildung oben***)
- o ***Gelesene Nachrichten ausblenden*** – Aktivieren Sie diesen Eintrag, um gelesene Nachrichten nicht mehr anzuzeigen, so dass neue Nachrichten nachrücken können
- o ***Schaltfläche zeigt an*** – In diesem Feld können Sie die Art der Neuigkeiten auswählen, die in der Neuigkeiten-Übersicht der ***AVG Security Toolbar*** angezeigt werden sollen
  - – Klicken Sie auf diese Schaltfläche, um die Übersicht über Neuigkeiten zu schließen

8.1.6. Verlauf löschen

Über diese Schaltfläche können Sie den Browserverlauf löschen, genauso wie über die Option ***AVG-Logo -> Verlauf löschen***.

8.1.7. eMail-Benachrichtigung

Über die Schaltfläche ***eMail-Benachrichtigung*** können Sie die Option aktivieren, über neue eMail-Nachrichten direkt in der Benutzeroberfläche der ***AVG Security Toolbar*** benachrichtigt zu werden. Durch Klicken auf diese Schaltfläche wird der folgende Bearbeitungsdialog angezeigt, in dem Sie Parameter für Ihr eMail-Konto und Anzeigeregeln für eMails festlegen können. Folgen Sie den Anweisungen im Dialog:



- ***Kontotyp*** – Geben Sie den verwendeten Protokolltyp Ihres eMail-Kontos an. Folgende



Optionen stehen zur Auswahl: *Google Mail*, *POP3*, oder wählen Sie aus dem Dropdown-Menü die Option *Andere* aus, um den Servernamen anzugeben (*verwenden Sie diese Option, wenn Sie ein eMail-Konto von Yahoo! JP Mail oder Hotmail besitzen*). Wenn Sie sich nicht sicher sind, welchen eMail-Servertyp Ihr Konto verwendet, wenden Sie sich an Ihren eMail-Anbieter oder Internetdienstanbieter.

- ***Login*** – Geben Sie in dem nachfolgenden Bereich Ihre *eMail-Adresse* und Ihr *Kennwort* ein. Behalten Sie die Aktivierung der Option *Automatischer Login* bei, so dass Sie die Daten nicht erneut eingeben müssen.
- ***Konto prüfen*** – Verwenden Sie diese Schaltfläche, um die eingegeben Daten zu testen.
- ***Einstellungen zurücksetzen*** – Entfernt schnell die oben eingegebene eMail-Adresse.
- ***Auf neue eMails überprüfen alle ... Minuten*** – Geben Sie das Zeitintervall an, in dem auf neue eMails überprüft werden soll (*zwischen 5 und 120 Minuten*), und geben Sie an, ob und wie Sie über neue Nachrichten informiert werden möchten.
- ***Meldungen bei neuen eMails zulassen*** – Heben Sie diese Markierung auf, um die visuelle Benachrichtigung beim Eingang neuer eMail-Nachrichten zu deaktivieren.
    - ***Ton bei Eingang neuer eMails abspielen*** – Heben Sie diese Markierung auf, um eine Audio-Meldung bei Eingang neuer eMails zu deaktivieren.
    - ***Benachrichtigungsfenster nach 5 Sekunden schließen*** – Markieren Sie diese Option, damit das Benachrichtigungsfenster beim Eingang neuer eMail-Nachrichten nach 5 Sekunden automatisch geschlossen wird.

8.1.8. Wetterinformationen

Über die Schaltfläche ***Wetter*** werden Informationen zum aktuellen Wetter (*wird alle 3–6 Stunden aktualisiert*) in Ihrer ausgewählten Region direkt in der ***AVG Security Toolbar*** angezeigt. Klicken Sie auf die Schaltfläche, um ein neues Informationsfenster mit einer genauen Wetterübersicht zu öffnen:





Die folgenden Bearbeitungsoptionen stehen zur Verfügung:

- ***Ort wechseln*** – Klicken Sie auf den Text ***Ort wechseln***, um einen neuen Dialog mit dem Titel ***Ort suchen*** anzuzeigen. Geben Sie den Namen des gewünschten Ortes in das Textfeld ein, und klicken Sie auf ***Suchen***. Wählen Sie in der Liste aller Ortsnamen den gesuchten Ort aus. Daraufhin wird das Informationsfenster mit Wetterinformationen zum gewünschten Ort angezeigt.

- ***Fahrenheit-/Celsius-Umrechner*** – Im oberen rechten Bereich des Informationsfenster können Sie zwischen der Fahrenheit- und der Celsius-Skala auswählen. Die Temperaturinformationen werden daraufhin in der ausgewählten Skala angezeigt.

- ***Ausführliche Vorhersage*** – Wenn Sie eine ausführliche Vorhersage wünschen, klicken Sie auf den Link ***Ausführliche Vorhersage***, und Sie werden zur spezialisierten Wetterseite weitergeleitet.

8.1.9. Facebook

Über die Schaltfläche ***Facebook*** können Sie das soziale Netzwerk Facebook direkt über die ***AVG Security Toolbar*** aufrufen. Klicken Sie auf diese Schaltfläche, und ein Login-Bestätigungsfenster wird angezeigt. Klicken Sie erneut auf die Schaltfläche, um den Login-Bildschirm von ***Facebook*** anzuzeigen. Geben Sie Ihre Anmeldedaten ein, und klicken Sie auf ***Anmelden***. Wenn Sie noch kein Konto bei Facebook besitzen, können Sie Ihr Konto direkt über den Link ***Für Facebook registrieren*** erstellen.

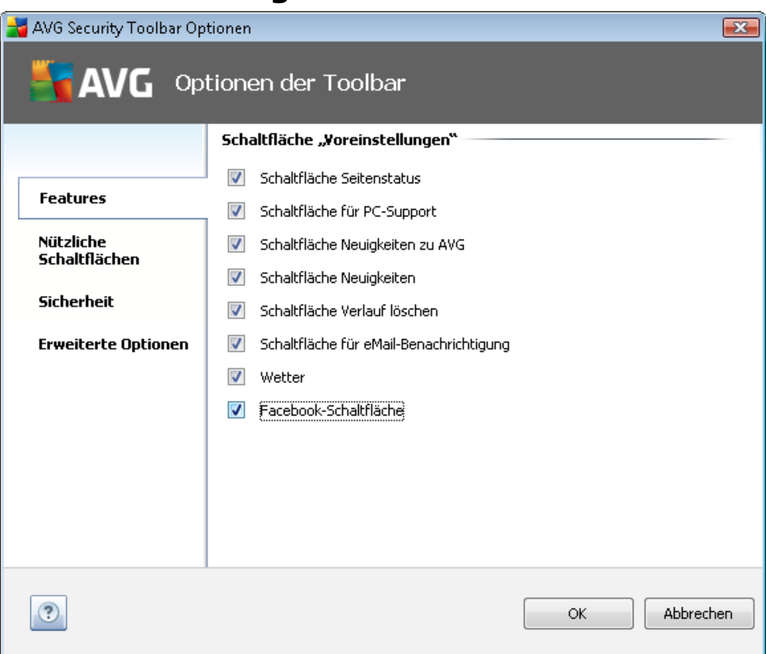
Nachdem Sie den Registrierungsvorgang bei Facebook abgeschlossen haben, werden Sie aufgefordert, die Anwendung ***AVG-Erweiterung für soziale Netzwerke*** zuzulassen. Wir empfehlen, diese Anwendung zuzulassen, da sie für die Verbindung mit Facebook über die Toolbar benötigt wird. Wenn Sie diese Anwendung zulassen, wird die Verbindung mit Facebook aktiviert, und die Schaltfläche ***Facebook*** wird in der ***AVG Security Toolbar*** angezeigt, die daraufhin über die Standardmenüoptionen von Facebook verfügt.



8.2. Optionen der AVG Security Toolbar

Alle Parameter der ***AVG Security Toolbar*** können Sie direkt im Bereich ***AVG Security Toolbar*** konfigurieren. Mit dem Menüeintrag *AVG / Optionen* der Toolbar wird die Bearbeitungsoberfläche in einem Dialog namens ***Optionen der Toolbar*** geöffnet, der aus vier Bereichen besteht:

8.2.1. Reiter „Allgemein"



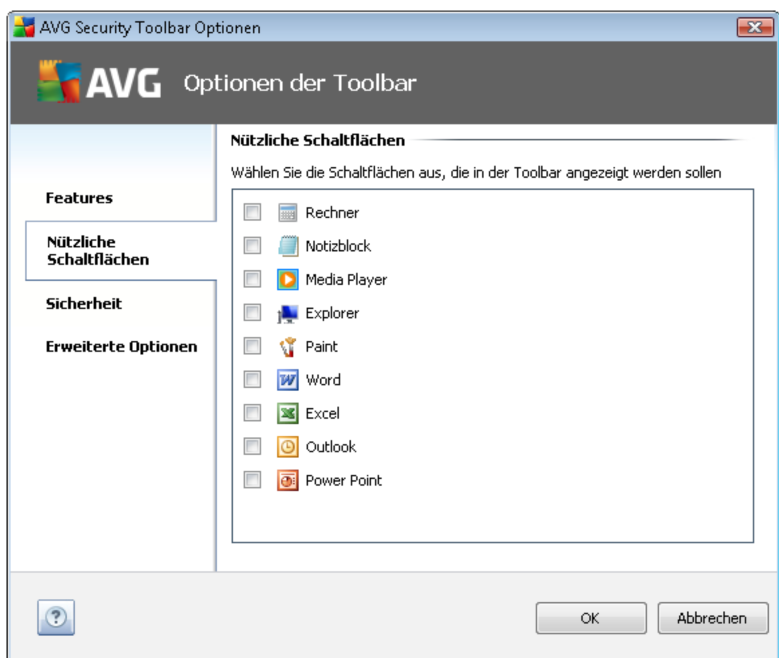
Auf diesem Reiter können Sie die Schaltflächen für die Toolbar-Steuerung festlegen, die im Bereich ***AVG Security Toolbar*** angezeigt bzw. ausgeblendet werden soll. Aktivieren Sie für die jeweils gewünschte Schaltfläche die entsprechende Option. Im Folgenden werden die Funktionen der einzelnen Toolbar-Schaltflächen beschrieben:

- ***Seitenstatus –*** Über diese Schaltfläche können Sie direkt in der ***AVG Security Toolbar***
- ***AVG Neuigkeiten*** – Öffnet die Webseite mit den neuesten Pressemitteilungen über AVG
- ***Neuigkeiten*** – Bietet eine strukturierte Übersicht über aktuelle Neuigkeiten aus der täglichen Presse
- ***Schaltfläche „Verlauf löschen"*** – Mit dieser Schaltfläche können Sie den Gesamten Verlauf löschen oder den Suchverlauf löschen, Browserverlauf löschen, Download-Verlauf löschen oder Cookies löschen – und zwar direkt im Bereich AVG Security Toolbar
- ***Schaltfläche für eMail-Benachrichtigung*** – Über diese Schaltfläche können Sie direkt in der ***AVG Security Toolbar*** Ihre neu eingegangenen eMails anzeigen
- ***Wetter*** – Über diese Schaltfläche erhalten Sie aktuelle Wetterinformationen zur ausgewählten Region



* ***Facebook*** – Über diese Schaltfläche können Sie direkt eine Verbindung mit dem sozialen Netzwerk Facebook herstellen

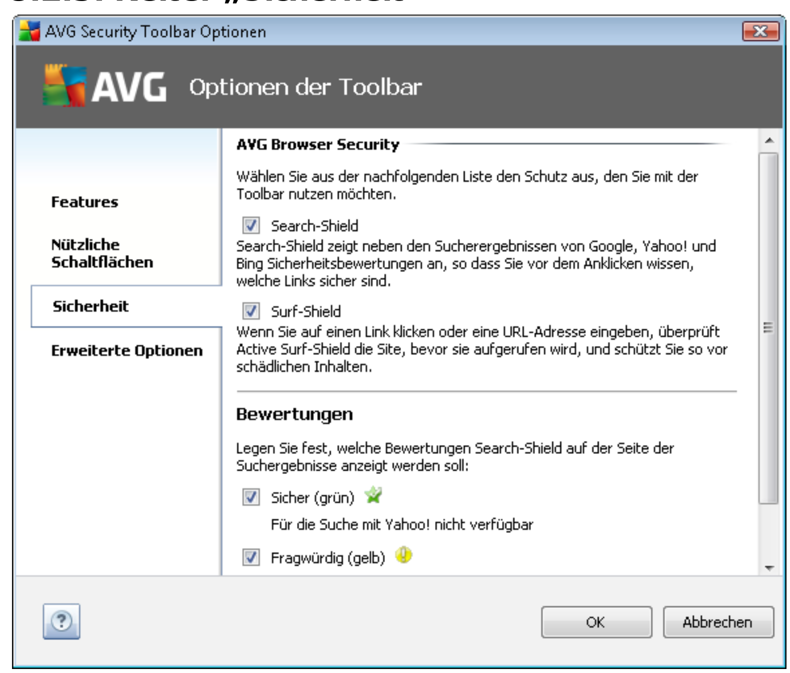
8.2.2. Reiter „Nützliche Schaltflächen“



Über den Reiter ***Nützliche Schaltflächen*** können Sie Anwendungen aus einer Liste auswählen, um deren Symbol in der Toolbar-Benutzeroberfläche anzuzeigen. Das Symbol fungiert dann als Quick Link, über den die entsprechende Anwendung sofort gestartet werden kann.



8.2.3. Reiter „Sicherheit“



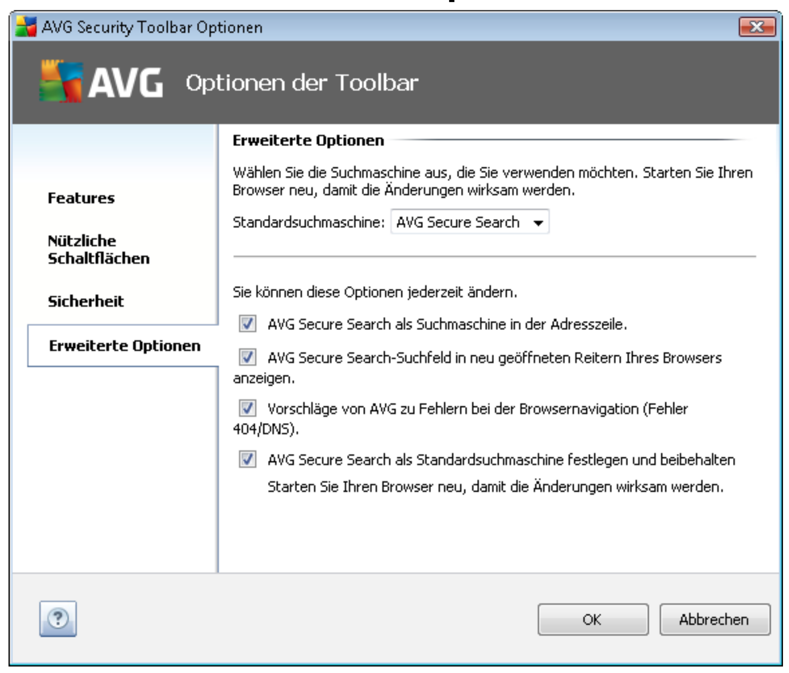
Der Reiter ***Sicherheit*** besteht aus zwei Bereichen, ***AVG Browser Security*** und ***Bewertungen***, wo Sie einzelne Kontrollkästchen aktivieren können, um Funktionen der ***AVG Security Toolbar*** zuzuweisen, die Sie verwenden möchten:

- ***Browser Security*** – Aktivieren Sie diesen Eintrag, um das ***AVG Search-Shield*** und/oder ***Surf-Shield*** zu aktivieren oder zu deaktivieren
- ***Bewertungen*** – Wählen Sie grafische Symbole aus, die das ***Search-Shield*** zur Bewertung von Suchergebnissen verwenden soll:
    - Die Seite ist sicher
    - Die Seite ist leicht verdächtig
    - Die Seite umfasst Links zu wirklich gefährlichen Seiten
    - Die Seite enthält aktive Bedrohungen
    - Auf die Seite kann nicht zugegriffen werden. Darum konnte sie nicht gescannt werden

Markieren Sie die gewünschte Option, um zu bestätigen, dass Sie über diese Bedrohungsstufe informiert werden möchten. Die Anzeige der roten Markierung, die für Seiten mit aktiven und gefährlichen Bedrohungen steht, kann nicht deaktiviert werden. ***Auch hier empfehlen wir Ihnen, die Standardkonfiguration des Programmherstellers beizubehalten, solange Sie nicht einen guten Grund für eine Änderung haben.***



8.2.4. Reiter „Erweiterte Optionen"



Wählen Sie auf dem Reiter ***Erweiterte Optionen*** zunächst die gewünschte Standardsuchmaschine aus. Sie haben die Wahl zwischen *AVG Secure Search (powered by Google), Baidu, WebHledani*, *Yandex und Yahoo! JP*. Starten Sie nach der Änderung der Standardsuchmaschine Ihren Browser neu, damit die Änderungen wirksam werden.

Zudem können Sie weitere spezielle Einstellungen der ***AVG Security Toolbar*** aktivieren oder deaktivieren *(der angegebene Titel bezieht sich auf die standardmäßigen AVG Secure Search (powered by Google)-Einstellungen)*:

- ***Festlegen AVG Secure Search (powered by Google)als Suchanbieter für die Adressleiste*** – Wenn diese Option aktiviert ist, können Sie Suchbegriffe direkt in die Adresszeile Ihres Browsers eingeben und Google wird automatisch genutzt, um nach relevanten Websites zu suchen.

- ***Vorschläge von AVG zu Fehlern bei der Browsernavigation (Fehler 404/DNS)*** – Wenn Sie bei der Suche im Internet auf eine nicht vorhandene Seite bzw. eine Seite stoßen, die nicht angezeigt werden kann (Fehler 404), werden Sie automatisch auf eine Webseite mit einer Übersicht mit ähnlichen Seiten zum gesuchten Thema geleitet.

- ***Festlegen AVG Secure Search (powered by Google)als Standard-Suchanbieter*** – Google ist die Standardsuchmaschine für die Suche im Internet mit der ***AVG Security Toolbar***; durch die Aktivierung dieser Option wird diese Suchmaschine auch als Standardsuchmaschine Ihres Webbrowsers verwendet.

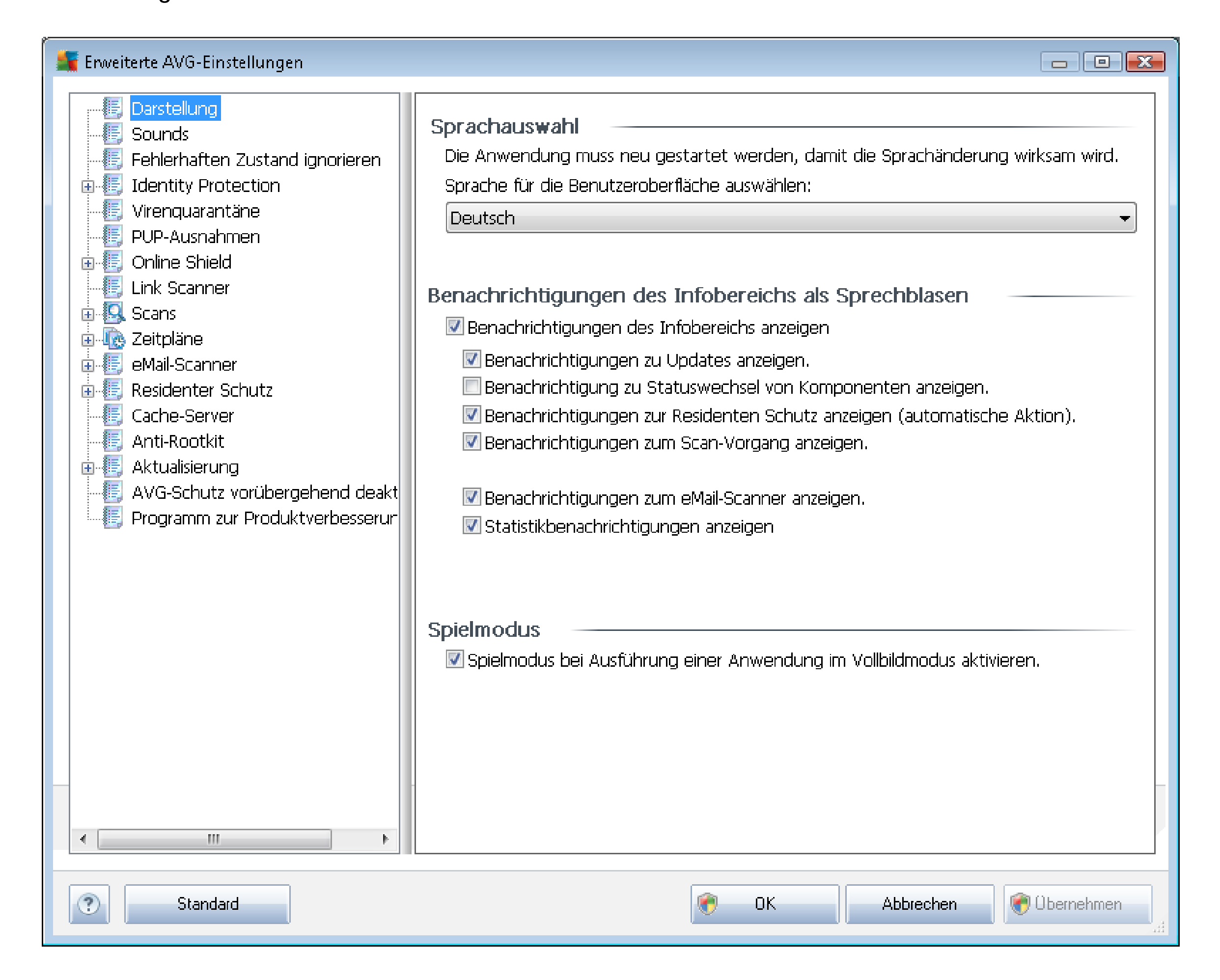


9. Erweiterte Einstellungen von AVG

Der Dialog zur erweiterten Konfiguration von **AVG Anti-Virus 2011** wird in einem neuen Fenster mit dem Namen ***Erweiterte AVG-Einstellungen*** geöffnet. Das Fenster ist in zwei Bereiche unterteilt: Der linke Bereich enthält eine Baumstruktur zur Navigation durch die Konfigurationsoptionen. Wählen Sie die Komponente (*oder den Teil einer Komponente*) aus, deren Konfiguration Sie ändern möchten, um den entsprechenden Bearbeitungsdialog im rechten Bereich des Fensters zu öffnen.

9.1. Darstellung

Der erste Eintrag der Baumstruktur, ***Darstellung***, bezieht sich auf die allgemeinen Einstellungen der Benutzeroberfläche von AVG und auf einige grundlegende Optionen für das Verhalten der Anwendung:



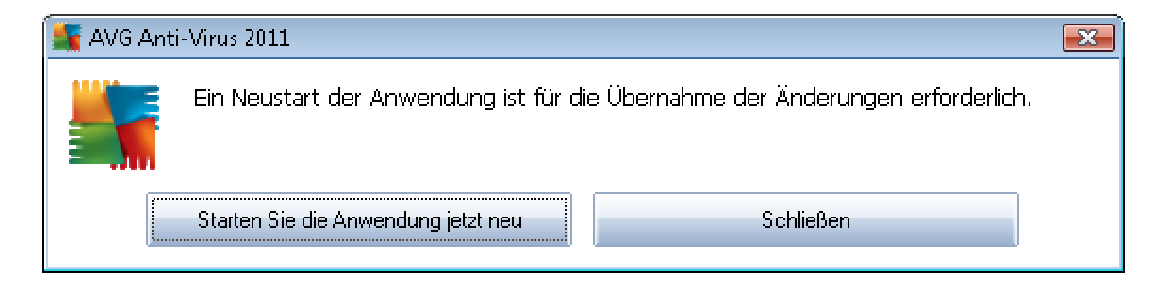
Sprachauswahl

Im Bereich ***Sprachauswahl*** kann aus dem Dropdown-Menü die gewünschte Sprache ausgewählt werden. Diese Sprache wird dann für die gesamte Benutzeroberfläche von AVG verwendet. Im Dropdown-Menü sind nur die Sprachen verfügbar, die zuvor beim Installationsvorgang ausgewählt wurden (*siehe Kapitel Benutzerdefinierte Optionen*) sowie die Benutzersprache Englisch (*wird*



standardmäßig installiert). Um den Wechsel zur ausgewählten Sprache abzuschließen, müssen Sie die Benutzeroberfläche wie folgt neu starten:

- Wählen Sie die gewünschte Sprache aus, und bestätigen Sie Ihre Auswahl mit der Schaltfläche ***Übernehmen*** (rechte untere Ecke)
- Klicken Sie zum Bestätigen auf die Schaltfläche ***OK***
- Es wird ein Dialog angezeigt, in dem Sie darüber informiert werden, dass nach einer Sprachänderung der Benutzeroberfläche von AVG ein Neustart der Anwendung erforderlich ist:



Benachrichtigungen des Infobereichs als Sprechblasen

In diesem Bereich können Sie die Anzeige von Benachrichtigungen des Infobereichs als Sprechblasen über den Status der Anwendung deaktivieren. Standardmäßig wird die Anzeige dieser Sprechblasen zugelassen, und es wird empfohlen, diese Konfiguration beizubehalten! Die Benachrichtigungen in den Sprechblasen enthalten meist Informationen über Statusänderungen der einzelnen Komponenten von AVG und sollten daher beachtet werden!

Wenn Sie dennoch möchten, dass diese Benachrichtigungen nicht angezeigt werden oder dass nur bestimmte Benachrichtigungen (zu einer bestimmten Komponente von AVG) angezeigt werden, können Sie dies durch Aktivierung/Deaktivierung der folgenden Optionen festlegen:

- ***Benachrichtigungen des Infobereichs anzeigen*** – Diese Option ist standardmäßig (*aktiviert*), so dass die Benachrichtigungen angezeigt werden. Wenn Sie die Markierung dieser Option aufheben, wird die Anzeige von Benachrichtigungen in Sprechblasen vollständig deaktiviert. Wenn diese Funktion aktiviert ist, können Sie auswählen, welche Benachrichtigungen angezeigt werden sollen:
    - ***Benachrichtigungen des Infobereichs zu [Updates](#)*** anzeigen – Legen Sie fest, ob Informationen zum Start, Fortschritt und Abschluss des Aktualisierungsvorgangs von AVG angezeigt werden sollen;
    - ***Benachrichtigungen zum Statuswechsel von Komponenten anzeigen*** – Legen Sie fest, ob Informationen zur Aktivität/Inaktivität der Komponenten angezeigt werden sollen und ob Sie über auftretende Probleme informiert werden möchten. Die Option zur Benachrichtigung über den fehlerhaften Status einer Komponente entspricht der Informationsfunktion des [Infobereichsymbols](#), das (durch einen Farbwechsel) auf Probleme aufmerksam macht, die im Zusammenhang mit AVG-Komponenten auftreten;



- ***Benachrichtigungen des Infobereichs zu [Residenter Schutz] anzeigen (automatische Aktion)*** – Legen Sie fest, ob Informationen zum Speichern, Kopieren und Öffnen von Dateien angezeigt werden sollen (*diese Konfiguration zeigt an, ob die Option Automatisches Heilen des Residenten Schutzes aktiviert ist*);

- ***Benachrichtigungen des Infobereichs zum Scan-Vorgang*** anzeigen – Legen Sie fest, ob Informationen zum automatischen Start, Fortschritt und Abschluss des geplanten Scan-Vorgangs angezeigt werden sollen;

- ***Benachrichtigungen des Infobereichs zum eMail-Scanneranzeigen*** – Legen Sie fest, ob Informationen zur Überprüfung aller eingehenden und ausgehenden eMails angezeigt werden sollen.

- ***Statistische Benachrichtigungen anzeigen*** – Lassen Sie diese Option aktiviert, damit reguläre statistische Prüfbenachrichtigungen in der Taskleiste angezeigt werden.

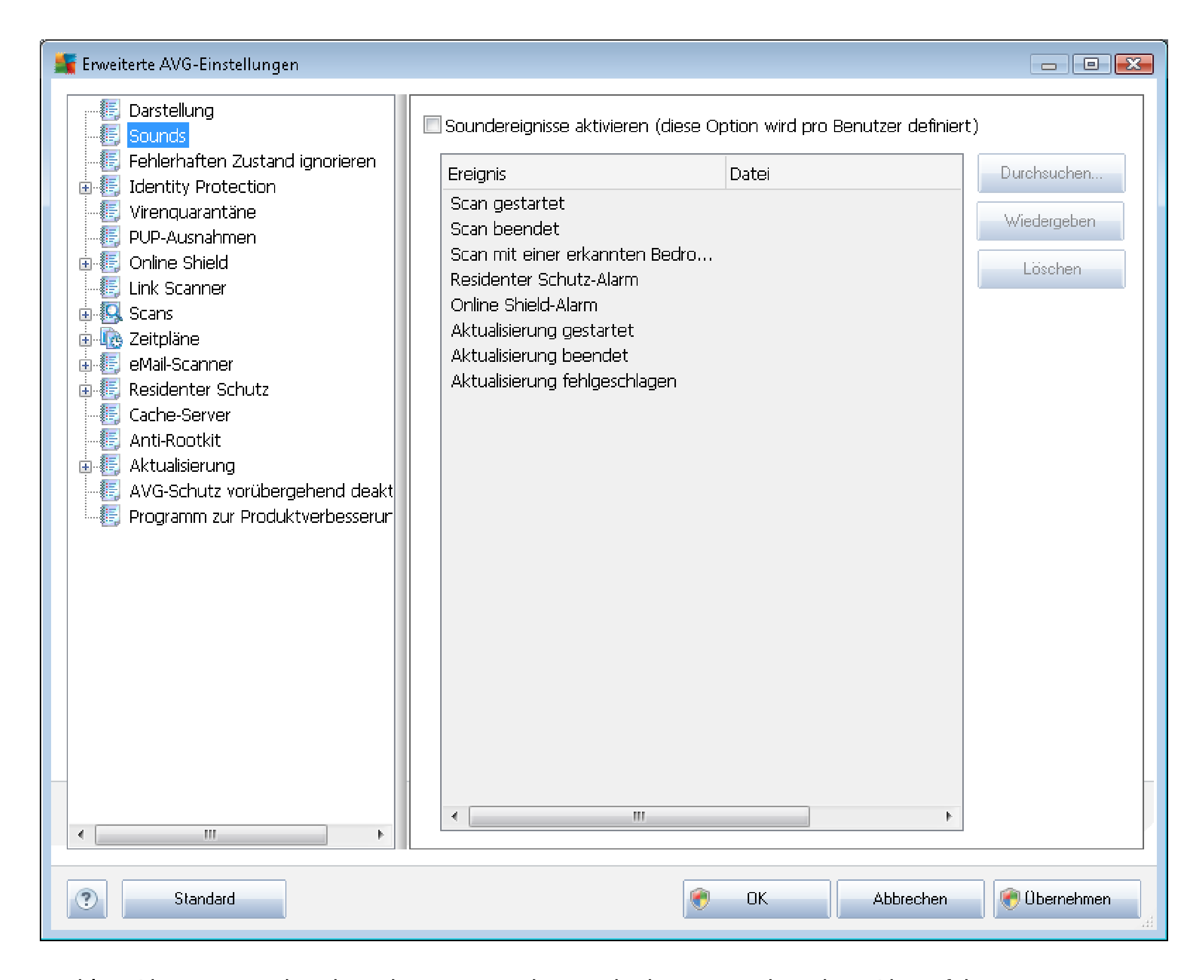
Spielmodus

Diese Funktion von AVG wurde für Anwendungen mit Vollbildmodus entwickelt, bei denen Informationsfenster von AVG (*z. B. beim Start eines geplanten Scans*) stören könnten (*eine Anwendung könnte minimiert oder ihre Grafiken könnten beschädigt werden*). Um dies zu vermeiden, sollten Sie das Kontrollkästchen ***Spielmodus bei Ausführung einer Anwendung im Vollbildmodus aktivieren*** aktiviert lassen (*Standardeinstellung*).

9.2. Sounds

Im Dialog ***Sounds*** können Sie festlegen, ob Sie bei bestimmten Aktionen von AVG per Soundbenachrichtigung informiert werden möchten. Wenn ja, aktivieren Sie die Option ***Soundereignisse aktivieren*** (*standardmäßig deaktiviert*), um die Liste der Aktionen von AVG zu aktivieren:





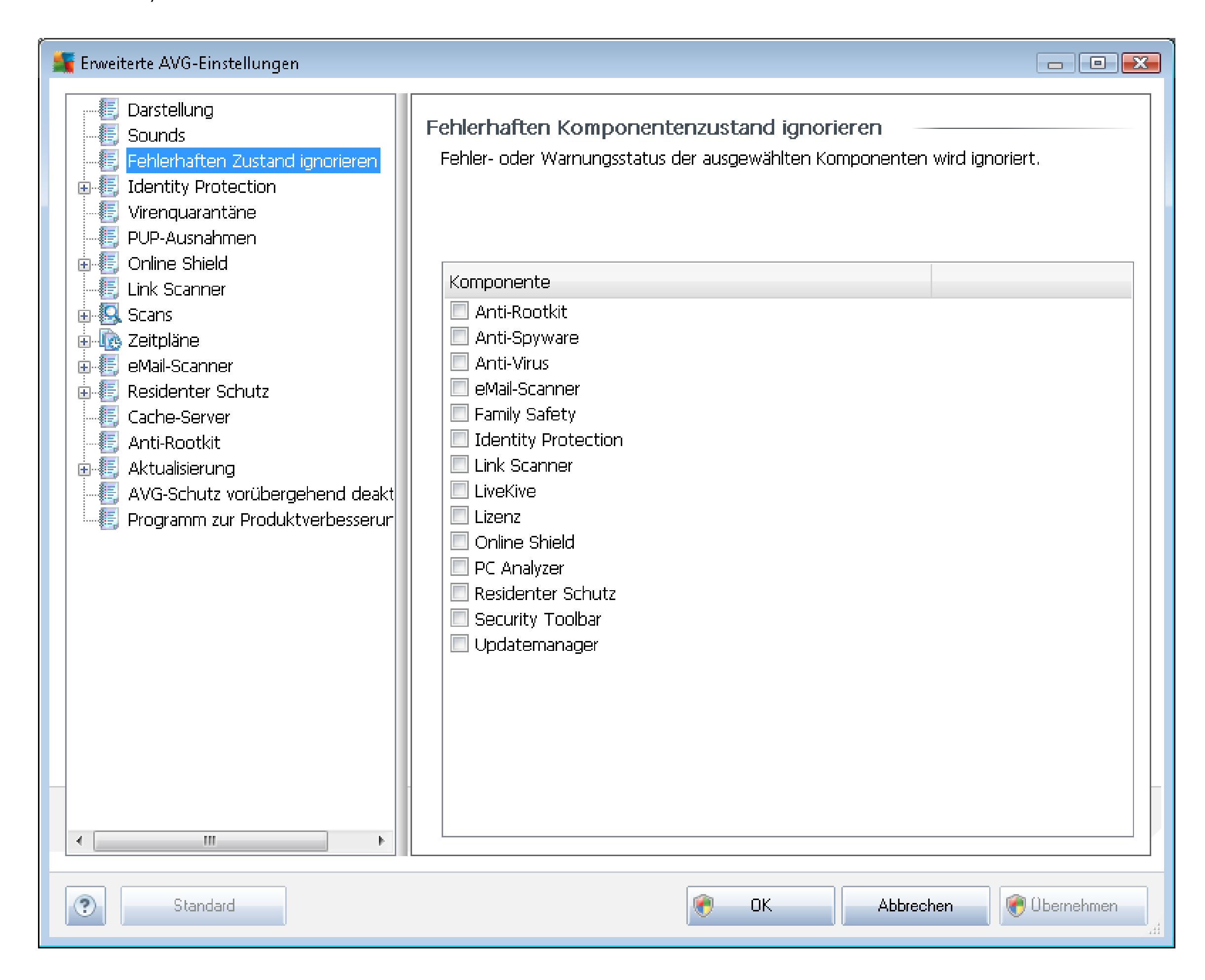
Wählen Sie nun aus der Liste das gewünschte Ereignis aus, und suchen Sie auf Ihrem Datenträger nach einem Sound (***Durchsuchen***), den Sie diesem Ereignis zuweisen möchten. Um den ausgewählten Sound anzuhören, markieren Sie das Ereignis in der Liste, und klicken Sie auf die Schaltfläche ***Wiedergeben*** . Verwenden Sie die Schaltfläche ***Löschen***, um den einem Ereignis zugewiesenen Sound zu entfernen.

Hinweis: *Es werden ausschließlich Sounds vom Typ *.wav unterstützt!*



9.3. Fehlerhaften Zustand ignorieren

Im Dialog ***Fehlerhaften Komponentenzustand ignorieren*** können Sie die Komponenten markieren, über die Sie nicht informiert werden möchten:



Standardmäßig sind alle Komponenten in dieser Liste deaktiviert. Das bedeutet: Wenn eine Komponente einen Fehlerstatus aufweist, erhalten Sie sofort eine Nachricht über das

- ***Symbol im Infobereich*** – Wenn alle Teile von AVG ordnungsgemäß funktionieren, wird das Symbol in vier Farben dargestellt. Tritt ein Fehler auf, wird das Symbol mit einem gelben Ausrufezeichen angezeigt

- und eine Beschreibung zum bestehenden Problem wird im Bereich ***Informationen zum Sicherheitsstatus*** im Hauptfenster von AVG angezeigt.

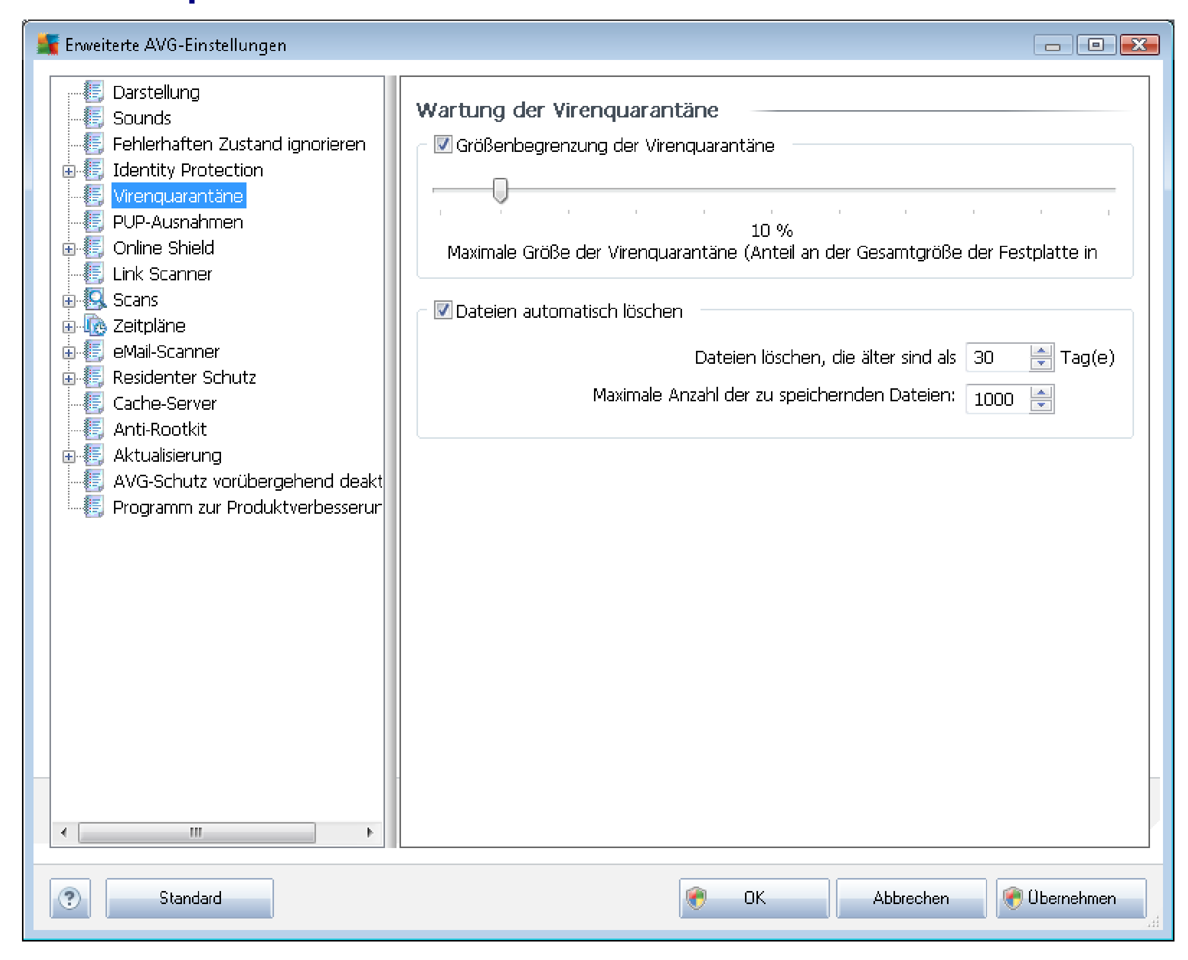
Es kann vorkommen, dass Sie aus bestimmten Gründen eine Komponente vorübergehend deaktivieren möchten. (*Die Deaktivierung einer Komponente wird nicht empfohlen. Achten Sie darauf, dass alle Komponenten aktiviert und die jeweiligen Standardeinstellungen vorgenommen sind*). In diesem Fall zeigt das Symbol im Infobereich automatisch eine Nachricht zum Fehlerstatus der Komponente an. Dieser spezielle Fall stellt natürlich keinen Fehler im eigentlichen Sinne dar, da er von Ihnen absichtlich herbeigeführt wurde und Sie sich über das potentielle Risiko bewusst sind.



Sobald das Symbol grau angezeigt wird, kann es keine weiteren Fehler melden.

Für diesen Fall können Sie im oben angezeigten Dialog Komponenten auswählen, die eventuell einen fehlerhaften Status aufweisen (*oder deaktiviert sind*) oder über die Sie keine Informationen erhalten möchten. Alternativ steht für einige Komponenten die Option ***Komponentenstatus ignorieren*** zur Verfügung, die über die Komponentenübersicht im Hauptfenster von AVG festgelegt werden kann.

9.4. Virenquarantäne



Im Dialog ***Wartung der Virenquarantäne*** können Sie mehrere Parameter hinsichtlich der Verwaltung der in der ***Virenquarantäne*** gespeicherten Objekte festlegen:

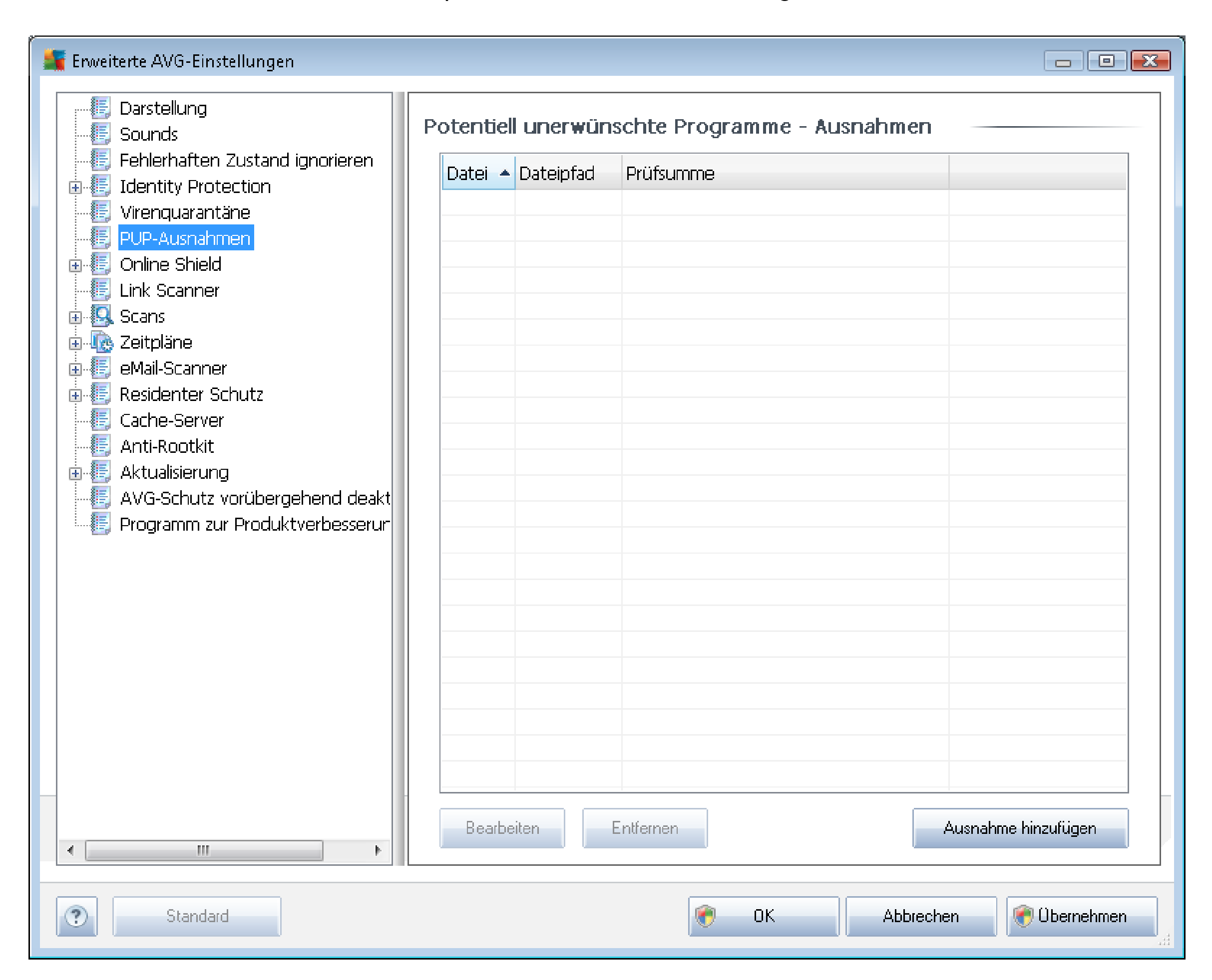
- ***Größenbegrenzung der Virenquarantäne*** – Mithilfe des Schiebereglers können Sie die maximale Größe der ***Virenquarantäne*** festlegen. Die Größe wird proportional zur Größe Ihrer lokalen Festplatte angegeben.

- ***Dateien automatisch löschen*** – In diesem Bereich wird die maximale Dauer festgelegt, die Objekte in der ***Virenquarantäne*** gespeichert werden (***Dateien löschen, die älter sind als ... Tage***), und die maximale Anzahl der in der ***Virenquarantäne*** gespeicherten Dateien (***Maximale Anzahl der zu speichernden Dateien***) bestimmt



9.5. PUP-Ausnahmen

AVG Anti-Virus 2011 ist in der Lage, ausführbare Anwendungen oder DLL-Bibliotheken, die im System potentiell unerwünscht sind, zu erkennen und zu analysieren. In bestimmten Fällen kann sich der Benutzer dazu entscheiden, unerwünschte Programme auf dem Computer zu belassen (*Programme, die absichtlich installiert worden sind*). Einige Programme (besonders kostenlose) enthalten Adware. Adware kann von AVG als ***potentiell unerwünschtes Programm*** erkannt und gemeldet werden. Wenn Sie ein derartiges Programm auf Ihrem Computer behalten möchten, können Sie es als Ausnahme eines potentiell unerwünschten Programms definieren:



Im Dialog ***Potentiell unerwünschten Programmen - Ausnahmen*** wird eine Liste der bereits definierten und aktuell gültigen Ausnahmen an potentiell unerwünschten Programmen angezeigt. Sie können die Liste bearbeiten, vorhandene Einträge löschen oder neue Ausnahmen hinzufügen. Für jede einzelne Ausnahme finden sich in der Liste die folgenden Angaben:

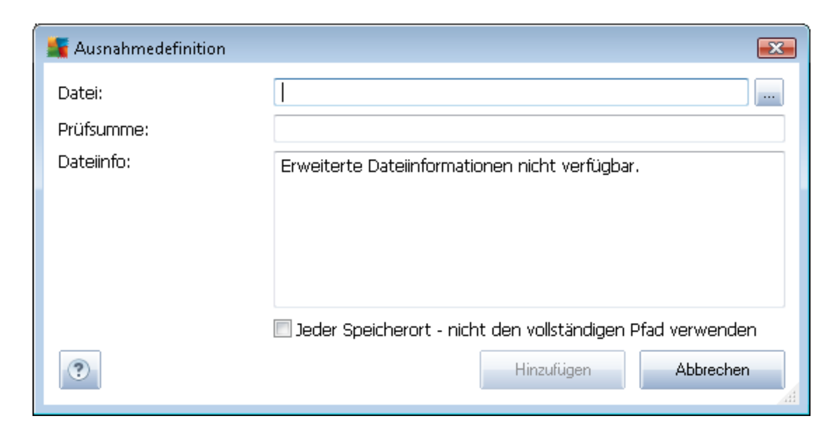
- ***Datei*** – Gibt den Namen der jeweiligen Anwendung an
- ***Dateipfad*** – Zeigt den Pfad zum Speicherort der Anwendung an
- ***Prüfsumme*** – Zeigt die eindeutige Signatur der ausgewählten Datei an. Bei der Prüfsumme handelt es sich um eine automatisch erzeugte Zeichenfolge, mit der AVG die ausgewählte



Datei eindeutig von anderen Dateien unterscheiden kann. Die Prüfsumme wird erzeugt und angezeigt, nachdem die Datei erfolgreich hinzugefügt wurde.

Schaltflächen

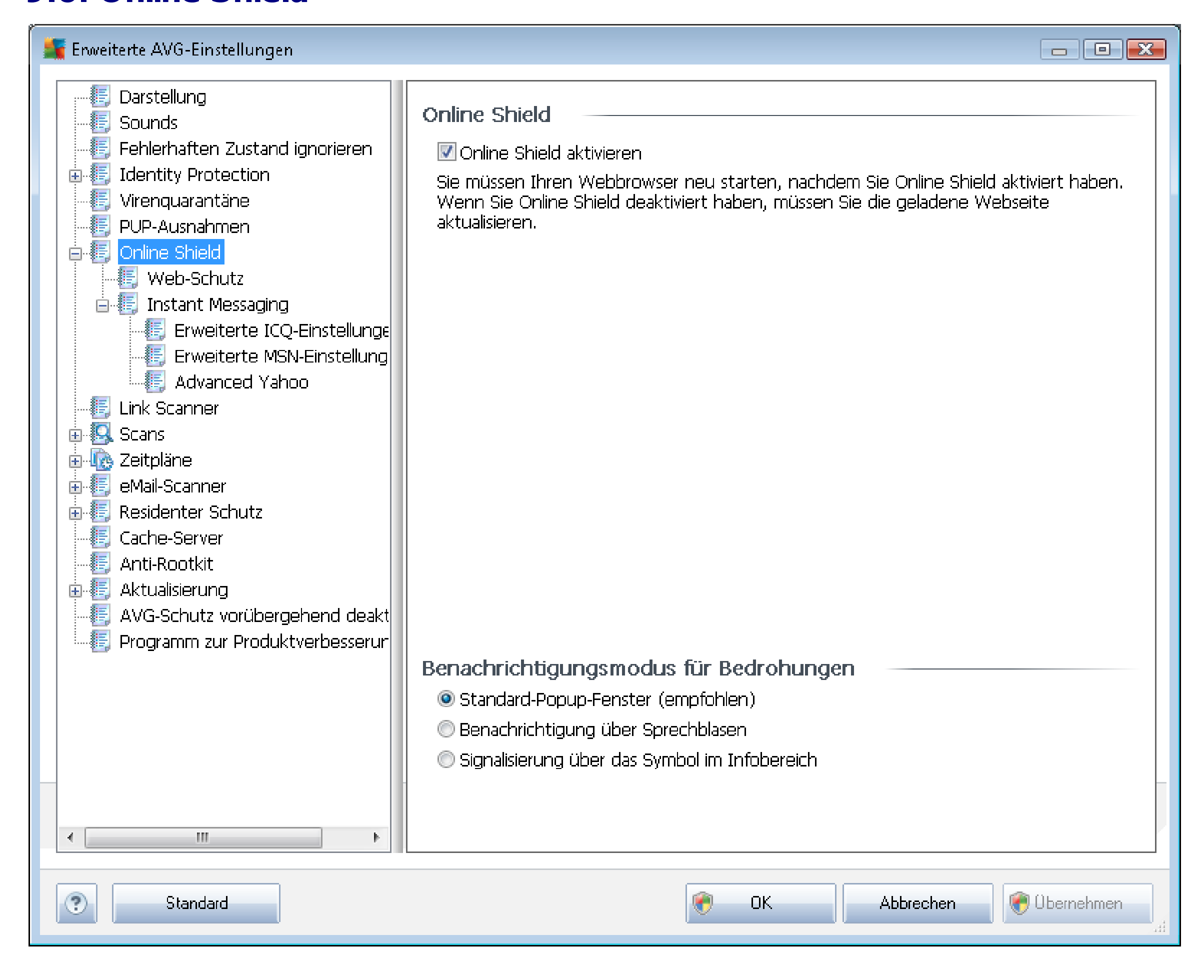
- ***Bearbeiten*** – Öffnet einen Bearbeitungsdialog (*der identisch ist mit dem Dialog für die Definition einer neuen Ausnahme; siehe unten*) einer bereits definierten Ausnahme, in dem Sie die Parameter der Ausnahme ändern können
- ***Entfernen***– Löscht das ausgewählte Element aus der Liste der Ausnahmen
- ***Ausnahme hinzufügen*** – Öffnet einen Bearbeitungsdialog, in dem Sie die Parameter der zu erstellenden neuen Ausnahme definieren können:



- o ***Datei*** – Geben Sie den vollständigen Pfad zu der Datei ein, die Sie als Ausnahme definieren möchten
- o ***Prüfsumme*** – Zeigt die eindeutige Signatur der ausgewählten Datei an. Bei der Prüfsumme handelt es sich um eine automatisch erzeugte Zeichenfolge, mit der AVG die ausgewählte Datei eindeutig von anderen Dateien unterscheiden kann. Die Prüfsumme wird erzeugt und angezeigt, nachdem die Datei erfolgreich hinzugefügt wurde.
- o ***Dateiinfo*** – Zeigt alle zusätzlichen Informationen über die Datei an (*Lizenz-/ Versionsdaten usw.*)
- o ***Jeder Speicherort – nicht den vollständigen Pfad verwenden*** – Wenn Sie diese Datei nur für diesen bestimmten Speicherort als Ausnahme festlegen möchten, lassen Sie das Kontrollkästchen deaktiviert. Wenn das Kontrollkästchen aktiviert ist, wird die angegebene Datei (unabhängig von ihrem Speicherort) als Ausnahme definiert (*Sie müssen trotzdem den vollständigen Pfad der Datei angeben; die Datei wird dann als Beispiel dafür verwendet, dass sich zwei Dateien mit demselben Namen auf Ihrem System befinden können*).



9.6. Online Shield



Im Dialog ***Online Shield*** können Sie die gesamte Komponente ***Online Shield*** mit der Option ***Online Shield aktivieren*** aktivieren bzw. deaktivieren (*standardmäßig aktiviert*). Erweiterte Einstellungen dieser Komponente finden Sie in den nachfolgenden Dialogen, die im Navigationsbaum aufgeführt werden:

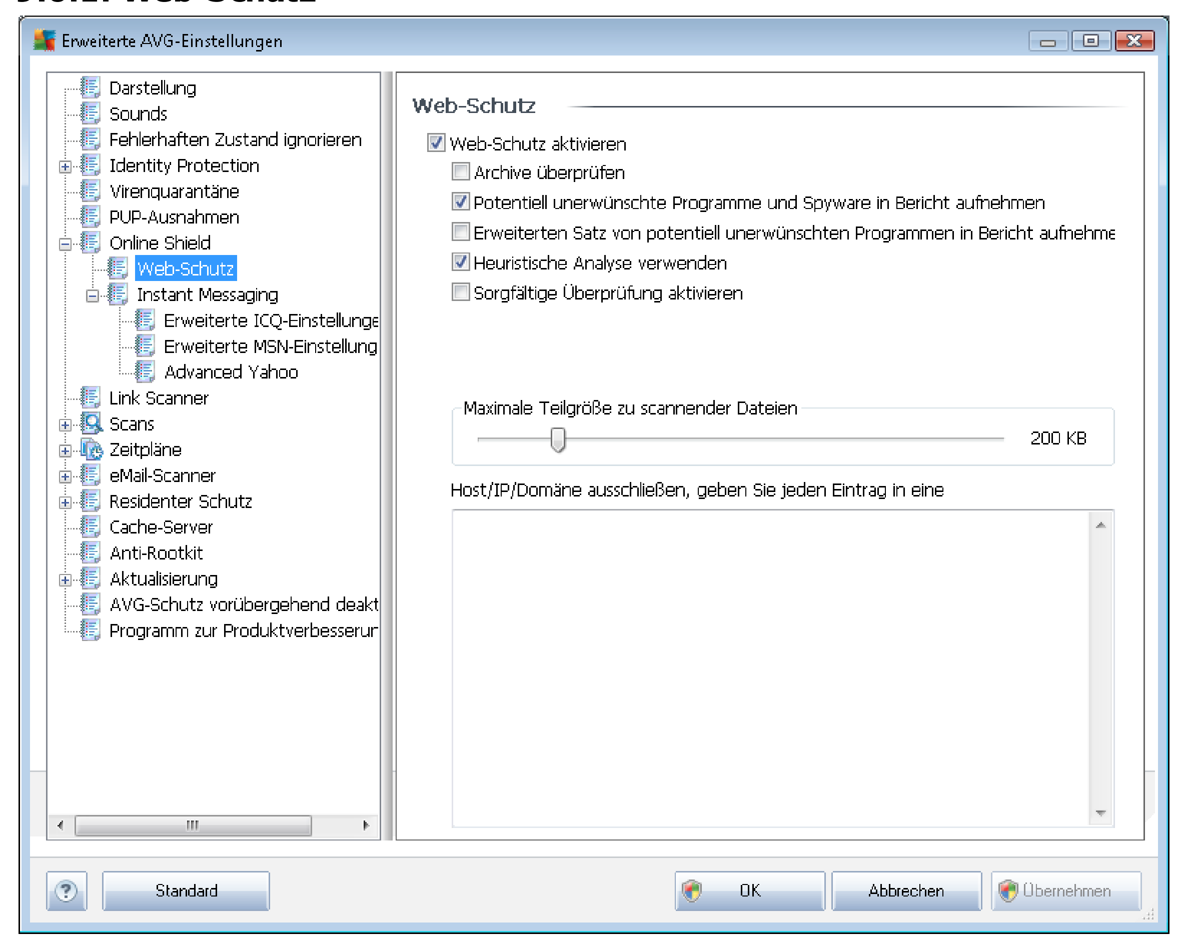
- ***Web-Schutz***
- ***Instant Messaging***

Benachrichtigungsmodus für Bedrohungen

Im unteren Bereich des Dialogs können Sie auswählen, wie Sie über mögliche Bedrohungen informiert werden möchten: mit einem Standard-Popup-Fenster, mit einer Benachrichtigung über Sprechblasen oder durch ein Symbol im Infobereich.



9.6.1. Web-Schutz



Im Dialog ***Web-Schutz*** können Sie die Konfiguration der Komponente hinsichtlich des Scans von Website-Inhalten bearbeiten. Auf der Bearbeitungsoberfläche können Sie die folgenden grundlegenden Optionen konfigurieren:

- ***Web-Schutz aktivieren*** – Mit dieser Option wird bestätigt, dass ***Online Shield*** die Inhalte von Seiten im Internet scannen soll. Wenn diese Option aktiviert ist (*standardmäßig aktiviert*), können Sie darüber hinaus folgende Elemente aktivieren/deaktivieren:
    - ***Archive überprüfen*** – (*standardmäßig deaktiviert*): Archivinhalte, die möglicherweise auf einer anzuzeigenden Webseite enthalten sind, werden ebenfalls gescannt.
    - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert*): Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.



- o ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** – (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- o ***Heuristische Analyse verwenden*** – (*standardmäßig aktiviert*): Der Inhalt der angezeigten Webseite wird mithilfe der Methode heuristische Analyse gescannt (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*).

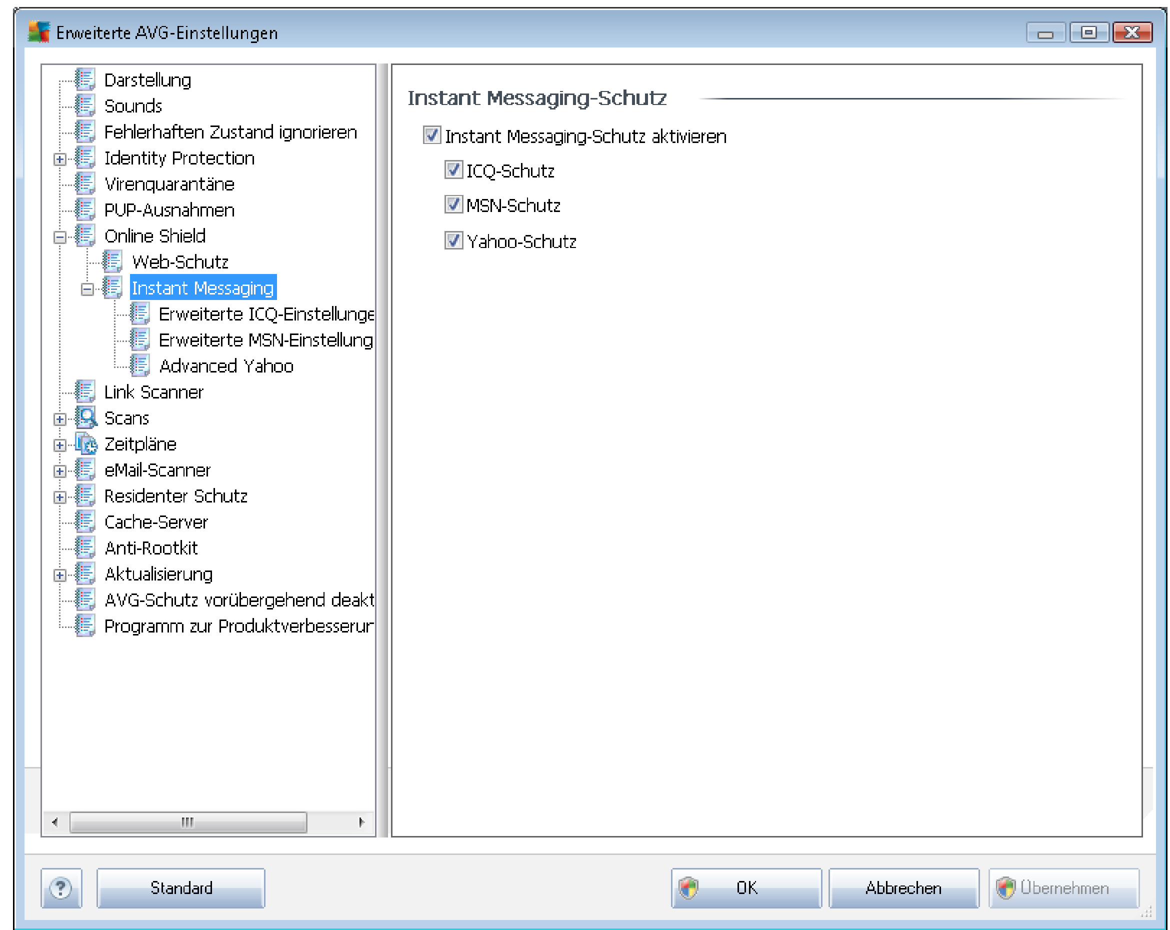
o ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

o ***Maximale Teilgröße zu scannender Dateien*** – Wenn die angezeigte Webseite Dateien enthält, können Sie deren Inhalte scannen, noch bevor diese auf Ihren Computer heruntergeladen werden. Das Scannen großer Dateien kann jedoch einige Zeit in Anspruch nehmen und das Herunterladen der Webseite ist signifikant langsamer. Mithilfe des Schiebereglers können Sie die maximale Größe einer Datei festlegen, die noch mit ***Online Shield*** gescannt werden soll. Selbst wenn die heruntergeladene Datei größer als festgelegt ist und daher nicht mit Online Shield gescannt wird, sind Sie weiterhin geschützt: Sollte die Datei infiziert sein, wird dies von ***Residenter Schutz*** sofort erkannt.

o ***Host/IP/Domäne ausschließen*** – In dieses Textfeld können Sie den genauen Namen eines Servers (*Host oder IP-Adresse, IP-Adresse mit Maske oder URL*) oder einer Domäne eingeben, die nicht von ***Online Shield*** *gescannt werden sollen.* Schließen Sie daher nur Hosts aus, die mit Sicherheit keine gefährlichen Webinhalte bereitstellen.



9.6.2. Instant Messaging



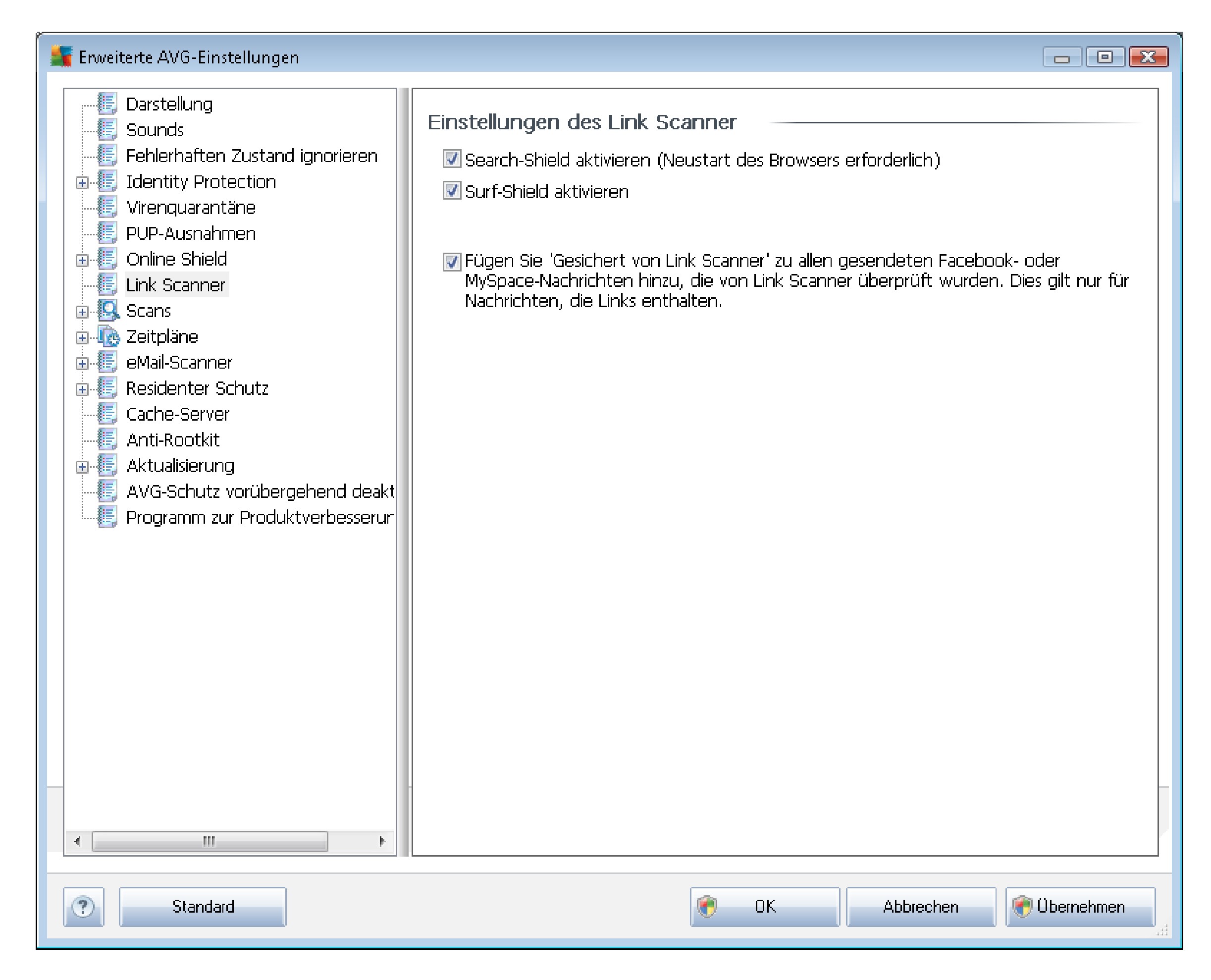
Im Dialog ***Instant Messaging-Schutz*** können Sie die Einstellungen der Komponente ***Online Shield*** im Zusammenhang mit dem Scannen von Instant Messaging bearbeiten. Momentan werden die folgenden drei Instant Messaging-Programme unterstützt: ***ICQ***, ***MSN*** und ***Yahoo*** – Aktivieren Sie die jeweiligen Einträge, wenn Sie möchten, dass ***Online Shield*** die Online-Kommunikation auf Viren überprüft.

Genaue Angaben zu zugelassenen/blockierten Benutzern können Sie im entsprechenden Dialog (***Erweiterte ICQ-Einstellungen***, ***Erweiterte MSN-Einstellungen und Erweiterte Yahoo-Einstellungen***) überprüfen und bearbeiten. Sie können auch eine ***Whitelist*** (*Liste der Benutzer, die mit Ihnen kommunizieren dürfen*) sowie eine ***Blacklist*** (*Benutzer, die gesperrt werden sollen*) festlegen.



9.7. Link Scanner

Im Dialog ***Einstellungen des Link Scanner***können Sie die Grundfunktionen von ***Link Scanner*** aktivieren oder deaktivieren:



- ***Search-Shield aktivieren*** – (*standardmäßig aktiviert*): Benachrichtigungssymbole zu Suchabfragen in Google, Yahoo! JP, WebHledani, Yandex, Baidu, Bing, AOL, AltaVista, EarthLink, Ask, Seznam, eBay, Twitter, Digg und Slashdot weisen darauf hin, dass der Inhalt der als Suchergebnis angezeigten Sites überprüft wurde.

- ***Surf-Shield*** aktivieren – (*standardmäßig aktiviert*): Aktiver (*Echtzeit*-) Schutz vor unbeabsichtigtem Zugriff auf Exploit-Sites. Die Verbindungsherstellung zu bekannten bösartigen Sites und deren schädlichem Inhalt wird blockiert, wenn der Benutzer diese Sites über einen Webbrowser (*oder eine andere HTTP-basierte Anwendung*) aufruft.

- ***„Gesichert von Link Scanner" hinzufügen*** – Aktivieren Sie diesen Eintrag, wenn Sie zu allen von ***Link Scanner*** überprüften Nachrichten, die einen Link enthalten und von Facebook oder MySpace gesendet wurden, eine Zertifizierungsbenachrichtigung hinzufügen möchten.



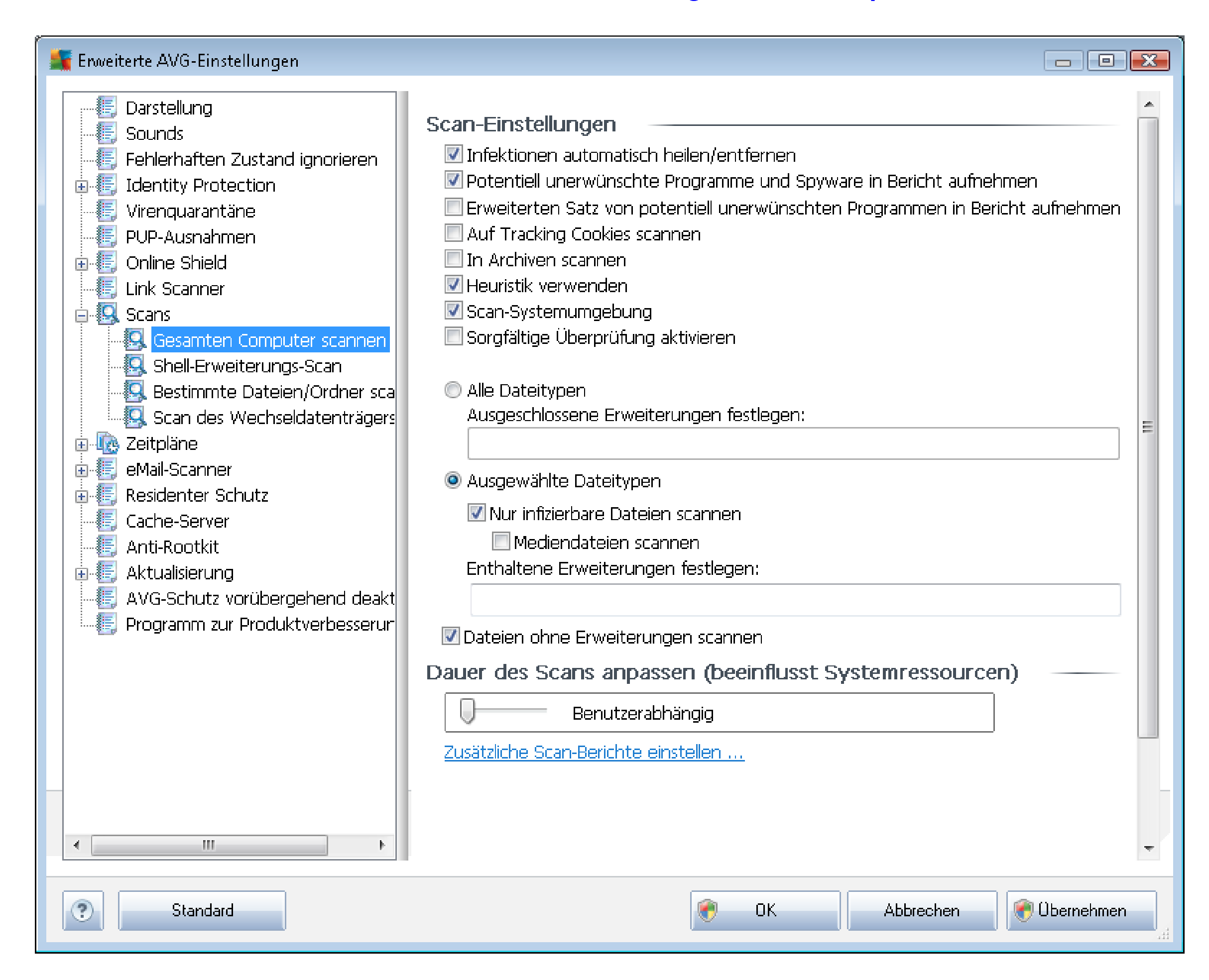
9.8. Scans

Die erweiterten Scan-Einstellungen sind in vier Kategorien eingeteilt, entsprechend den vom Software-Hersteller festgelegten Scan-Arten:

- ***Scan des gesamten Computers*** – Vordefinierter Standard-Scan des gesamten Computers
- ***Shell-Erweiterungs-Scan*** – Bestimmter Scan eines ausgewählten Objekts direkt von der Umgebung des Windows Explorer aus
- ***Bestimmte Dateien/Ordner scannen*** – Vordefinierter Standard-Scan ausgewählter Bereiche Ihres Computers
- ***Scan des Wechseldatenträgers*** – Bestimmter Scan der Wechseldatenträger, die an Ihren Computer angeschlossen sind

9.8.1. Gesamten Computer scannen

Mit der Option ***Scan des gesamten Computers*** können Sie die Parameter eines Scans bearbeiten, der vom Software-Hersteller vordefiniert wurde, ***Scan des gesamten Computers***:





Scan-Einstellungen

Im Bereich ***Scan-Einstellungen*** finden Sie eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können:

- ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die ***Virenquarantäne*** verschoben.
- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.
- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente Anti-Spyware legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).
- ***In Archiven scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.
- ***Heuristik verwenden*** (*standardmäßig aktiviert*) – Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet;
- ***Scan-Systemumgebung*** (*standardmäßig aktiviert*) – Beim Scan werden auch die Systembereiche Ihres Computers überprüft.
- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wird*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die kaum einer Infektion zum Opfer fallen. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

Außerdem sollten Sie entscheiden, welche Elemente gescannt werden



- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen (*beim Speichern werden ändern sich die Kommata in Semikola*), die nicht gescannt werden sollen;

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

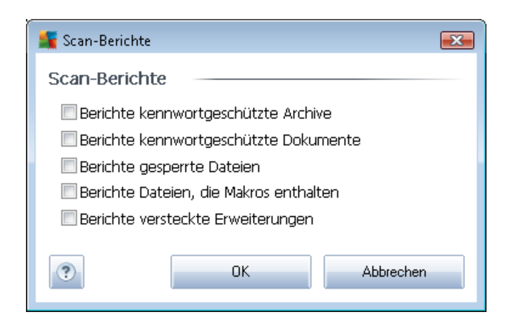
- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

Dauer des Scans anpassen

Im Bereich ***Dauer des Scans anpassen*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Wenn der Scan schneller ausgeführt werden soll, nimmt der Scan weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan ist aber deutlich erhöht, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*Diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber niemand daran arbeitet*). Auf der anderen Seite können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

Zusätzliche Scan-Berichte einstellen ...

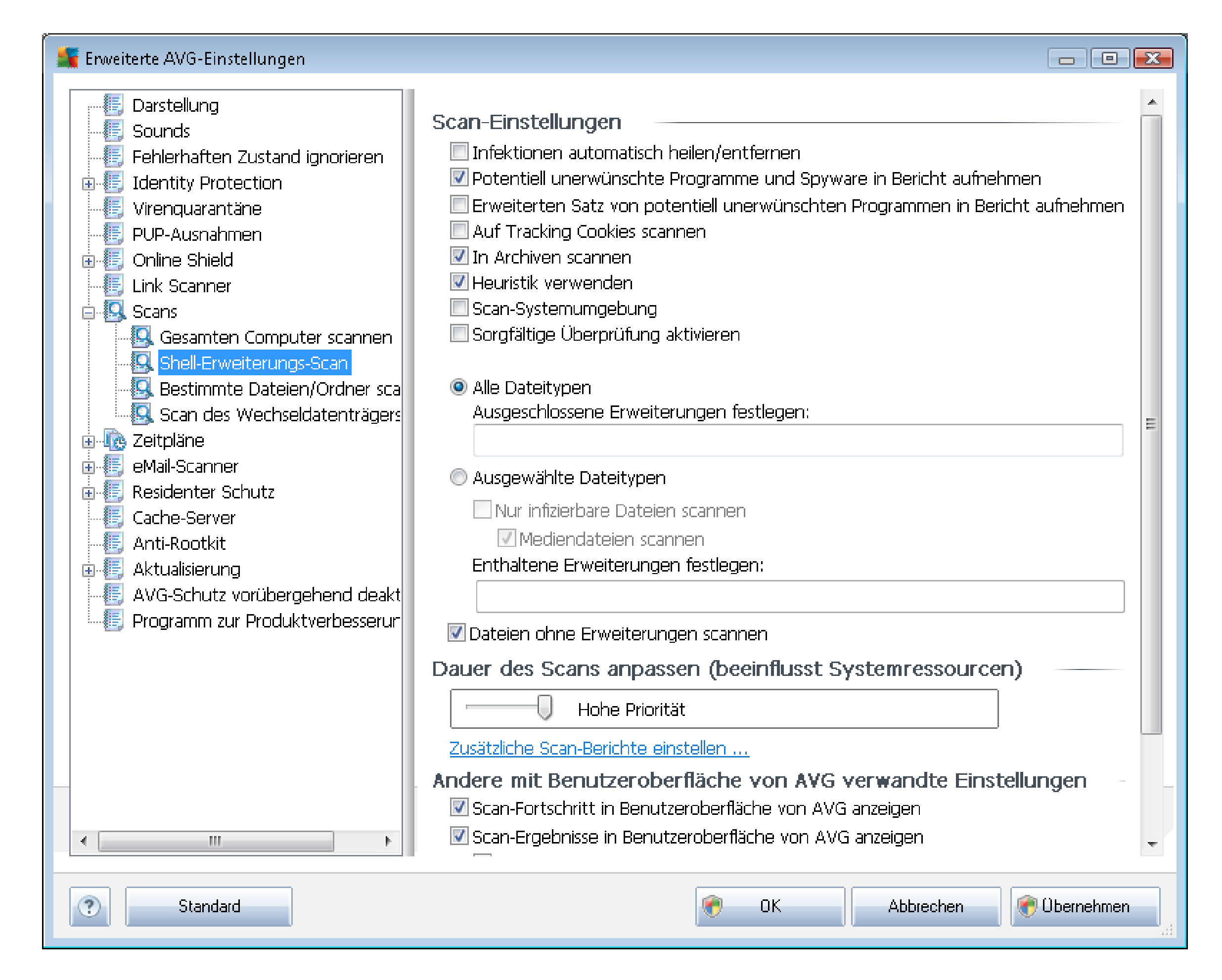
Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen ...***, um den separaten Dialog ***Scan-Berichte*** zu öffnen, wo Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



9.8.2. Shell-Erweiterungs-Scan

Ähnlich der vorhergehenden Option ***Scan des gesamten Computers*** enthält die Option ***Shell-Erweiterungs-Scan*** verschiedene Optionen zum Bearbeiten des vom Software-Hersteller vordefinierten Scans. Hier bezieht sich die Konfiguration auf das Scannen von bestimmten Objekten, das direkt von der Umgebung des Windows Explorer aus gestartet wird (*Shell-Erweiterung*). Siehe Kapitel ***Scans aus dem Windows Explorer***:





Die Parameterliste stimmt mit der Parameterliste der Option ***Gesamten Computer scannen*** überein. Die Standardeinstellungen unterscheiden sich jedoch: (*Während beim Scan des gesamten Computers standardmäßig keine Archive, aber die Systemumgebung gescannt wird, verhält es sich beim Shell-Extension-Scan umgekehrt*).

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***Erweiterte Einstellungen von AVG/Scans/Scan des gesamten Computers****.*

Im Vergleich zum Dialog ***Scan des gesamten Computers*** enthält der Dialog ***Shell-Erweiterungs-Scan*** auch den Bereich ***Andere Einstellungen bezüglich der Benutzeroberfläche von AVG***, in dem Sie festlegen können, dass der Scan-Fortschritt und Scan-Ergebnisse auch über die Benutzeroberfläche von AVG aufgerufen werden können. Sie können außerdem festlegen, dass Scan-Ergebnisse nur bei einer beim Scan erkannten Infektion angezeigt werden sollen.

9.8.3. Bestimmte Dateien/Ordner scannen

Die Bearbeitungsoberfläche für die Option ***Bestimmte Dateien/Ordner scannen*** stimmt mit dem Bearbeitungsdialog der Option ***Scan des gesamten Computers*** überein. Alle Konfigurationsoptionen sind gleich. Die Standardeinstellungen für die Option ***Gesamten Computer scannen*** sind jedoch strenger:



Erweiterte AVG-Einstellungen

- Darstellung
- Sounds
- Fehlerhaften Zustand ignorieren
- Identity Protection
- Virenquarantäne
- PUP-Ausnahmen
- Online Shield
- Link Scanner
- Scans
  - Gesamten Computer scannen
  - Shell-Erweiterungs-Scan
  - Bestimmte Dateien/Ordner sca
  - Scan des Wechseldatenträgers
- Zeitpläne
- eMail-Scanner
- Residenter Schutz
- Cache-Server
- Anti-Rootkit
- Aktualisierung
- AVG-Schutz vorübergehend deakt
- Programm zur Produktverbesserur

Scan-Einstellungen

- [x] Infektionen automatisch heilen/entfernen
- [x] Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen
- [ ] Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen
- [ ] Auf Tracking Cookies scannen
- [x] In Archiven scannen
- [x] Heuristik verwenden
- [ ] Scan-Systemumgebung
- [ ] Sorgfältige Überprüfung aktivieren

( ) Alle Dateitypen

Ausgeschlossene Erweiterungen festlegen:

(•) Ausgewählte Dateitypen

- [x] Nur infizierbare Dateien scannen
- [ ] Mediendateien scannen

Enthaltene Erweiterungen festlegen:

- [x] Dateien ohne Erweiterungen scannen

Dauer des Scans anpassen (beeinflusst Systemressourcen)

Benutzerabhängig

Zusätzliche Scan-Berichte einstellen ...

Standard | OK | Abbrechen | Übernehmen

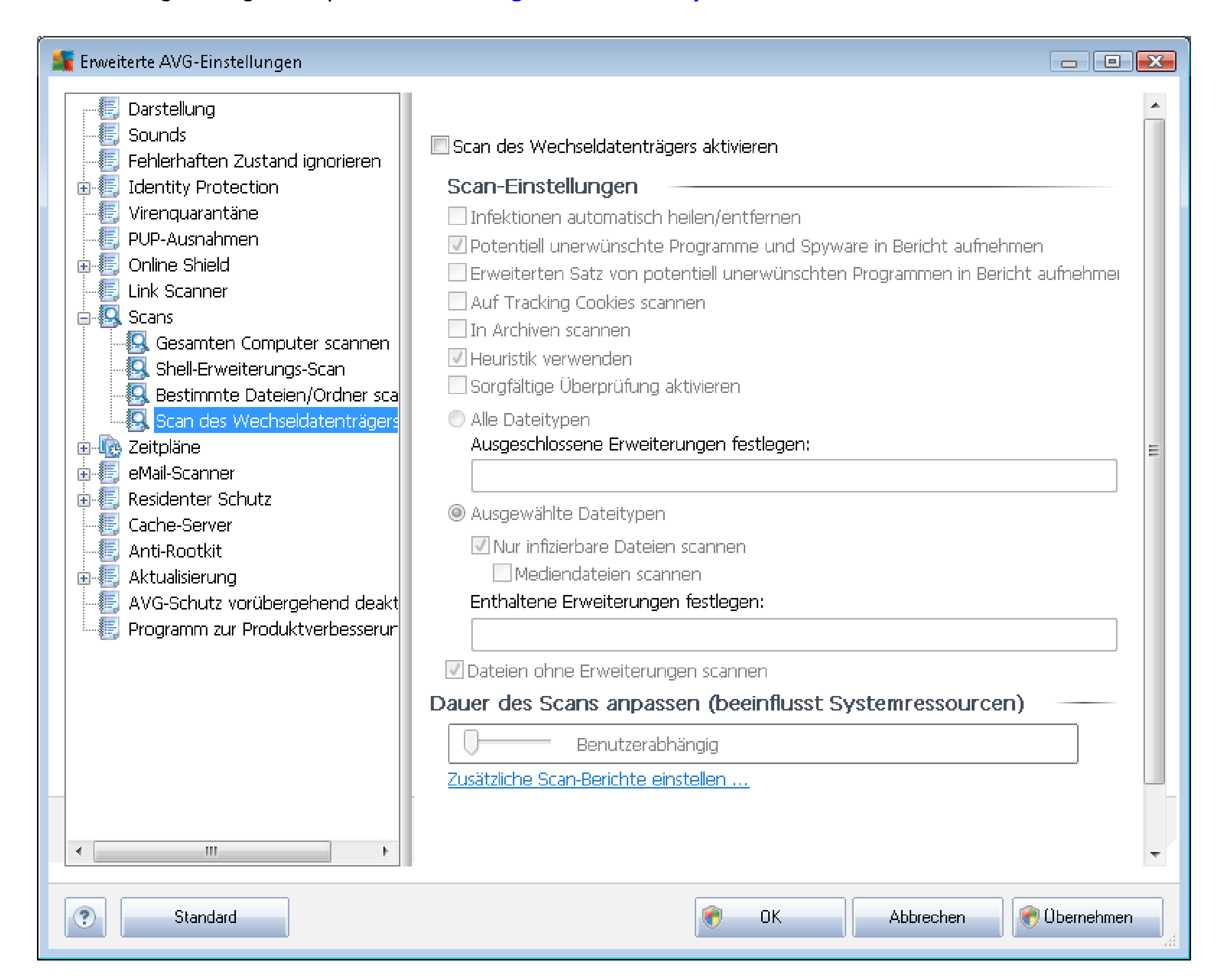
Alle Parameter, die in diesem Konfigurationsdialog festgelegt werden, gelten nur für die Scan-Bereiche, die unter der Option ***Bestimmte Dateien oder Ordner scannen*** ausgewählt wurden!

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***Erweiterte Einstellungen von AVG/Scans/Scan des gesamten Computers****.*



9.8.4. Scan des Wechseldatenträgers

Die Bearbeitungsoberfläche für die Option ***Scan des Wechseldatenträgers*** ist auch dem Bearbeitungsdialog der Option ***Scan des gesamten Computers*** sehr ähnlich:



Der ***Scan des Wechseldatenträgers*** wird automatisch gestartet, sobald Sie einen Wechseldatenträger an Ihren Computer anschließen. Standardmäßig ist der Scan deaktiviert. Es ist jedoch entscheidend, Wechseldatenträger auf potentielle Bedrohungen zu scannen, da diese die Hauptquelle von Infektionen sind. Aktivieren Sie das Kontrollkästchen ***Scan des Wechseldatenträgers aktivieren***, damit dieser Scan bereit ist und bei Bedarf automatisch gestartet werden kann.

Hinweis: *Eine Beschreibung der Parameter finden Sie im Kapitel* ***Erweiterte Einstellungen von AVG/Scans/Scan des gesamten Computers****.*

9.9. Zeitpläne

Im Bereich ***Zeitpläne*** können Sie die Standardeinstellungen für folgende Zeitpläne bearbeiten:

- Geplanter Scan



- [Zeitplan für Update der Virendatenbank]
- [Zeitplan für Update des Programms]

9.9.1. Geplanter Scan

Auf drei Reitern können die Parameter für den geplanten Scan bearbeitet (*oder ein neuer Zeitplan erstellt*) werden. Sie können den Eintrag ***Diese Aufgabe aktivieren*** auf jedem Reiter aktivieren oder deaktivieren, um den geplanten Test vorübergehend zu deaktivieren. Anschließend können Sie den Eintrag bei Bedarf hier wieder aktivieren:

Das Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) enthält den vom Programmhersteller zugewiesenen Namen für diesen Zeitplan. Bei neu hinzugefügten Zeitplänen (*Sie können einen neuen Zeitplan hinzufügen, indem Sie im linken Navigationsbaum mit der rechten Maustaste auf den Eintrag **Zeitplan für Update des Programms** klicken*) können Sie einen eigenen Namen angeben; in diesem Fall kann das Textfeld bearbeitet werden. Wählen Sie nach Möglichkeit kurze, beschreibende Namen für Ihre Scans, damit Sie die einzelnen Scans später leicht unterscheiden und wiederfinden können.

Beispiel: *Sie sollten einen Scan nicht „Neuer Scan“ oder „Mein Scan“ nennen, da diese Namen*



nichts darüber aussagen, was der Scan tatsächlich überprüft. Ein Beispiel für einen guten, beschreibenden Namen wäre andererseits „Scan von Systembereichen“ usw. Es ist auch nicht erforderlich, im Namen des Scans anzugeben, ob es sich um einen Scan des gesamten Computers handelt oder lediglich um den Scan bestimmter Dateien oder Ordner. Ihre eigenen Scans sind immer bestimmte Versionen eines Scans bestimmter Dateien oder Ordner.

In diesem Dialog können Sie weiterhin folgende Parameter für den Scan festlegen:

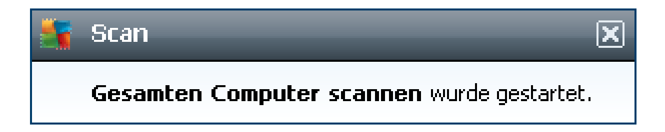
Zeitplan wird ausgeführt

Hier können Sie die Zeitintervalle für den Start des neu geplanten Scans festlegen. Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum (***Ausführung jede/n ...***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit ...***) oder ein Ereignis festlegen, das den Start eines Scans auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

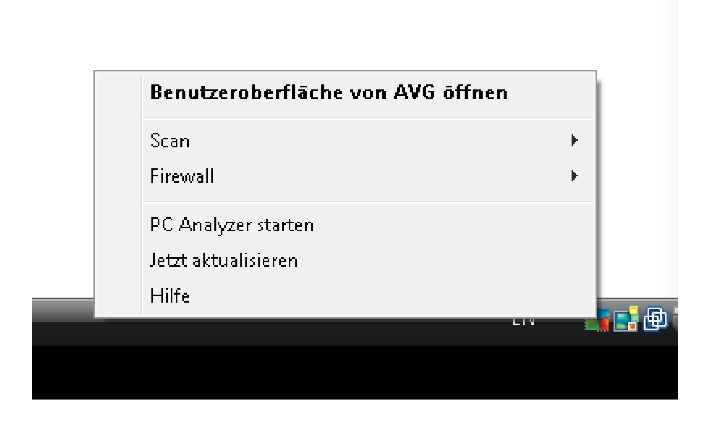
Erweiterte Zeitplanoptionen

In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist.

Sobald der geplante Scan zu der von Ihnen festgelegten Zeit startet, werden Sie darüber über ein Popup-Fenster informiert, das über dem AVG-Symbol im Infobereich geöffnet wird:



Daraufhin wird ein neues AVG-Symbol im Infobereich angezeigt (*in Vollfarbe und mit einer Ampel*), das Sie darauf hinweist, dass gerade ein geplanter Scan durchgeführt wird. Klicken Sie mit der rechten Maustaste auf das AVG-Symbol für einen laufenden Scan, um ein Kontextmenü zu öffnen, über das Sie den Scan unterbrechen oder auch anhalten können sowie die Priorität des momentan ausgeführten Scans ändern können.





Der Reiter ***Vorgehensweise beim Scannen*** enthält eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. Standardmäßig sind die meisten Parameter aktiviert, und ihre Funktionen werden während des Scans angewendet. Wenn Sie keinen wichtigen Grund haben, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten:

- ***Infektionen automatisch heilen/entfernen*** *(standardmäßig aktiviert):* Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die ***Virenquarantäne*** verschoben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** *(standardmäßig aktiviert):* ***Aktivieren Sie dieses Kontrollkästchen, um die Anti-Spyware*** -Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller



erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*): Dieser Parameter der Komponente ***Anti-Spyware*** legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*)

- ***In Archiven scannen*** (*standardmäßig deaktiviert*): Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

- ***Heuristik verwenden*** (*standardmäßig aktiviert*): Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet.

- ***Scan-Systemumgebung*** (*standardmäßig aktiviert*): Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***Auf Rootkits scannen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, wenn die Rootkit-Erkennung während des Scans des gesamten Computers durchgeführt werden soll. Die Rootkit-Erkennung kann über die Komponente ***Anti-Rootkit*** auch separat durchgeführt werden;

Außerdem sollten Sie entscheiden, welche Elemente gescannt werden

- ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen vom Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen (*beim Speichern ändern sich die Kommata in Semikola*), die nicht gescannt werden sollen;

- ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

- Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

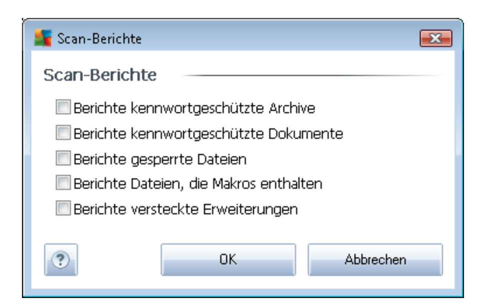


Dauer des Scans anpassen

Im Bereich ***Dauer des Scans anpassen*** können Sie die gewünschte Scan-Geschwindigkeit abhängig von der Nutzung der Systemressourcen festlegen. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Wenn der Scan schneller ausgeführt werden soll, nimmt der Scan zwar weniger Zeit in Anspruch, die Nutzung der Systemressourcen beim Scan liegt aber deutlich höher, und die anderen Aktivitäten auf dem Computer werden verlangsamt (*Diese Option sollten Sie verwenden, wenn Ihr Computer eingeschaltet ist, aber niemand daran arbeitet*). Auf der anderen Seite können Sie die Nutzung der Systemressourcen verringern, indem Sie die Scan-Dauer verlängern.

Zusätzliche Scan-Berichte einstellen

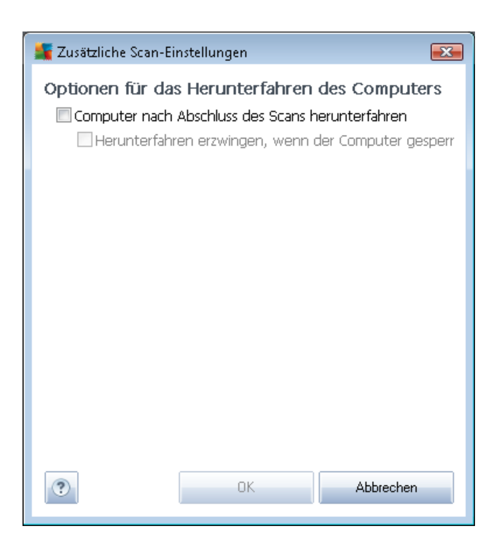
Klicken Sie auf den Link ***Zusätzliche Scan-Berichte einstellen ...***, um den separaten Dialog ***Scan-Berichte*** zu öffnen, wo Sie festlegen können, welche Scan-Ergebnisse berichtet werden sollen:



Zusätzliche Scan-Einstellungen

Klicken Sie auf ***Zusätzliche Scan-Einstellungen***, um einen neuen Dialog aufzurufen, in dem Sie Optionen für das Herunterfahren des Computers ***wählen können***. Legen Sie dort fest, ob der Computer nach dem Scan automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).





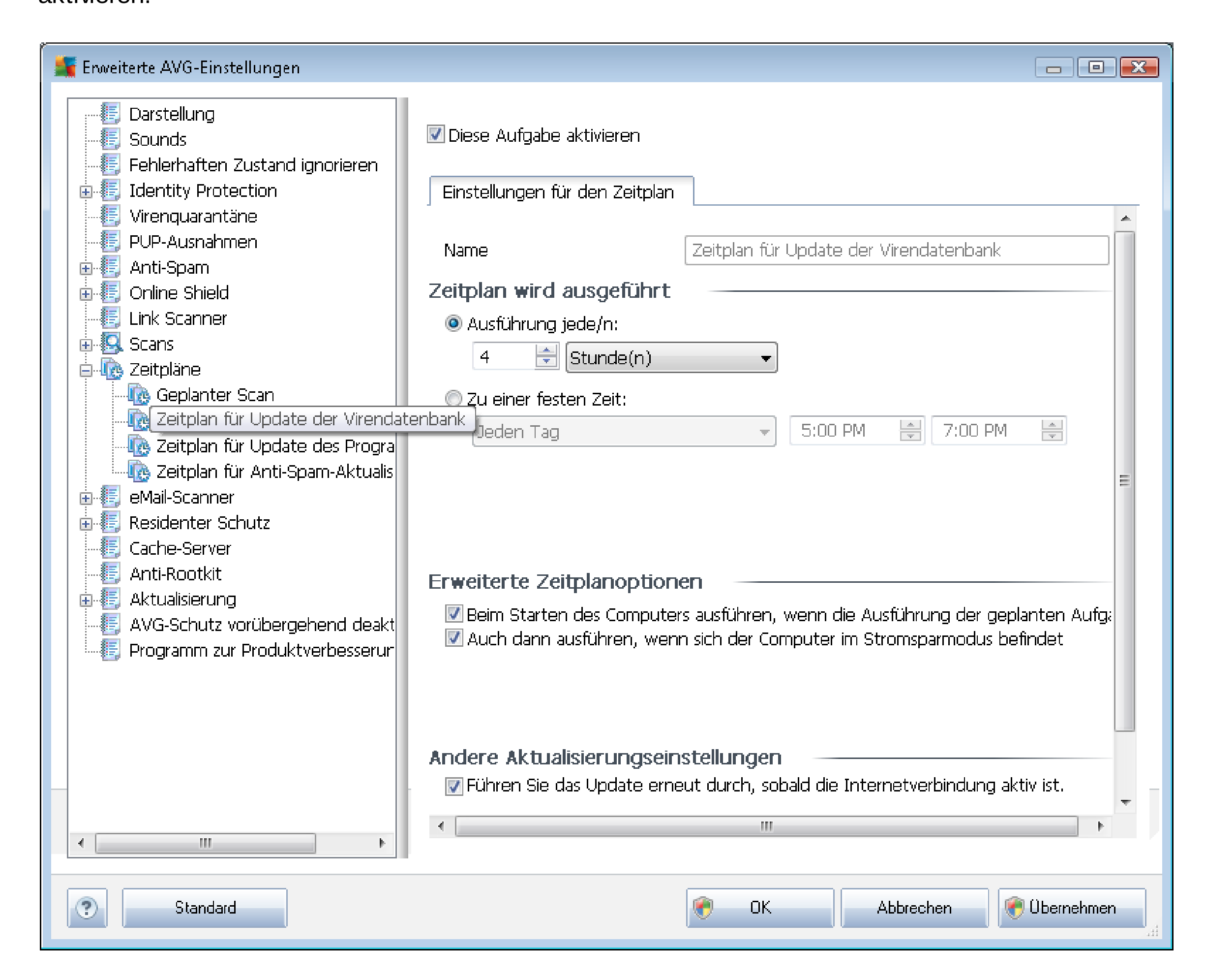
Auf dem Reiter ***Scan-Umfang*** können Sie festlegen, ob Sie die Option [Gesamten Computer scannen] oder [Bestimmte Dateien oder Ordner scannen] planen möchten. Wenn Sie die Option „Bestimmte Dateien oder Ordner scannen“ auswählen, wird im unteren Bereich dieses Dialogs die



angezeigte Baumstruktur aktiviert, und Sie können die zu scannenden Ordner festlegen.

9.9.2. Zeitplan für Update der Virendatenbank

Falls ***wirklich erforderlich***, können Sie den Eintrag ***Diese Aufgabe aktivieren*** deaktivieren, um das geplante Update der Virendatenbank vorübergehend zu deaktivieren bzw. später erneut zu aktivieren:



Der grundlegende Aktualisierungszeitplan der Virendatenbank erfolgt über die Komponente ***Updatemanager***. In diesem Dialog können Sie verschiedene Parameter des Aktualisierungszeitplans der Virendatenbank im Detail festlegen. Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

Zeitplan wird ausgeführt

Legen Sie in diesem Bereich die Zeitintervalle fest, in denen das neu geplante Update der Virendatenbank durchgeführt werden soll.
Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum (***Ausführung jede/n ...***) oder ein genaues Datum und eine Uhrzeit (***Ausführung zu einer bestimmten Zeit ...***)



festlegen.

Erweiterte Zeitplanoptionen

In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen die Virendatenbank aktualisiert werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder ganz ausgeschaltet ist).

Andere Aktualisierungseinstellungen

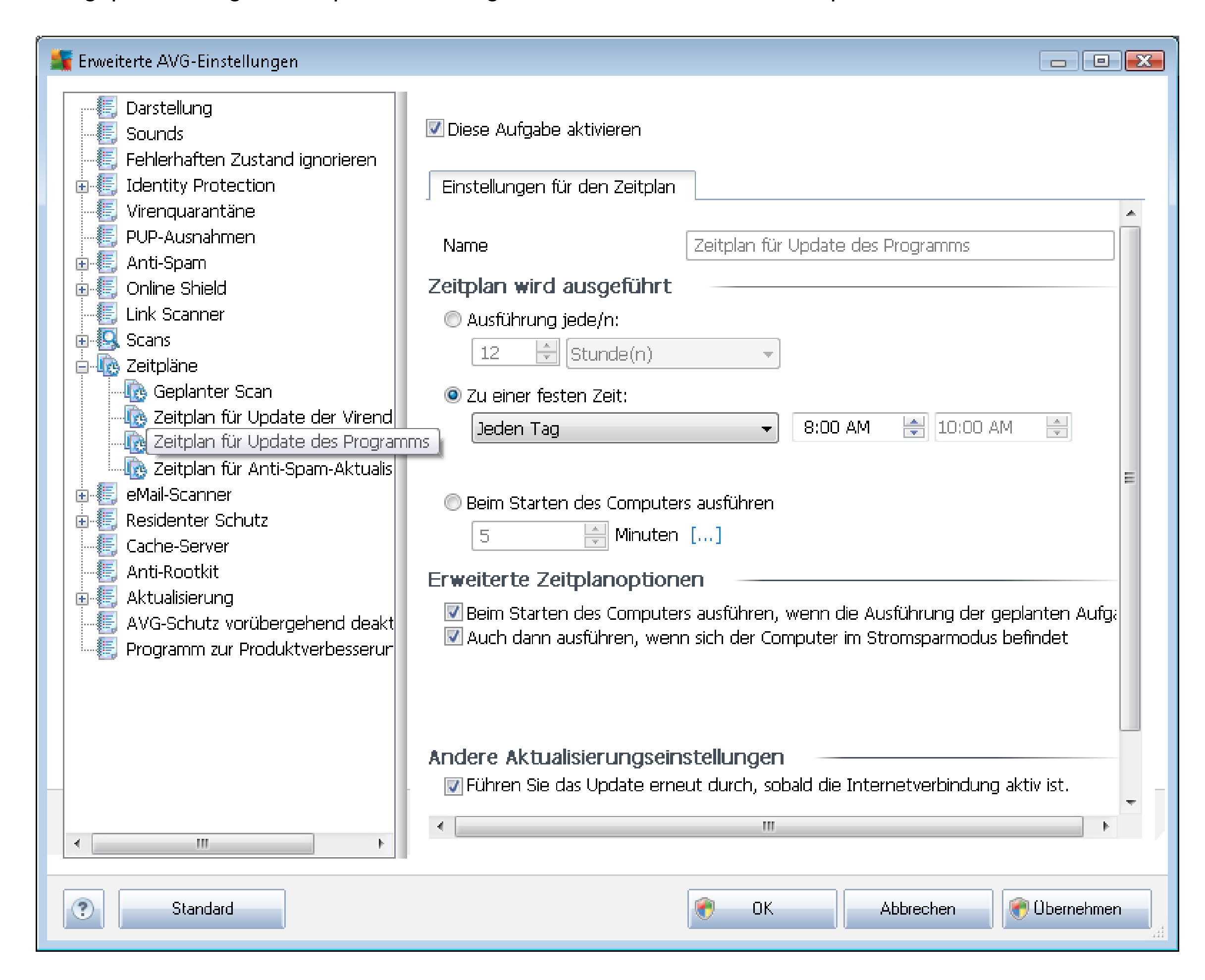
Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung neu gestartet wird.

Sobald das geplante Update zu der von Ihnen festgelegten Zeit startet, werden Sie darüber in einem Popup-Fenster informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog **Erweiterte Einstellungen/Darstellung** beibehalten)*.



9.9.3. Zeitplan für Update des Programms

Falls ***wirklich erforderlich***, können Sie den Eintrag ***Diese Aufgabe aktivieren*** deaktivieren, um das geplante Programm-Update vorübergehend zu deaktivieren bzw. später erneut zu aktivieren:



Im Textfeld mit dem Titel ***Name*** (*bei allen Standardzeitplänen deaktiviert*) finden Sie den Namen, den der Zeitplan vom Programmhersteller erhalten hat.

Zeitplan wird ausgeführt

Legen Sie hier die Zeitintervalle für das Ausführen des neu geplanten Programmupdates fest. Sie können entweder wiederholte Starts des Updates nach einem bestimmten Zeitraum (***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Updates auslösen soll (***In Abhängigkeit von einer bestimmten Aktion: Beim Start des Computers***).

Erweiterte Zeitplanoptionen

In diesem Abschnitt können Sie festlegen, unter welchen Bedingungen das Programmupdate



gestartet werden soll oder nicht (zum Beispiel wenn sich der Computer im Stromsparmodus befindet oder komplett ausgeschaltet ist).

Andere Aktualisierungseinstellungen

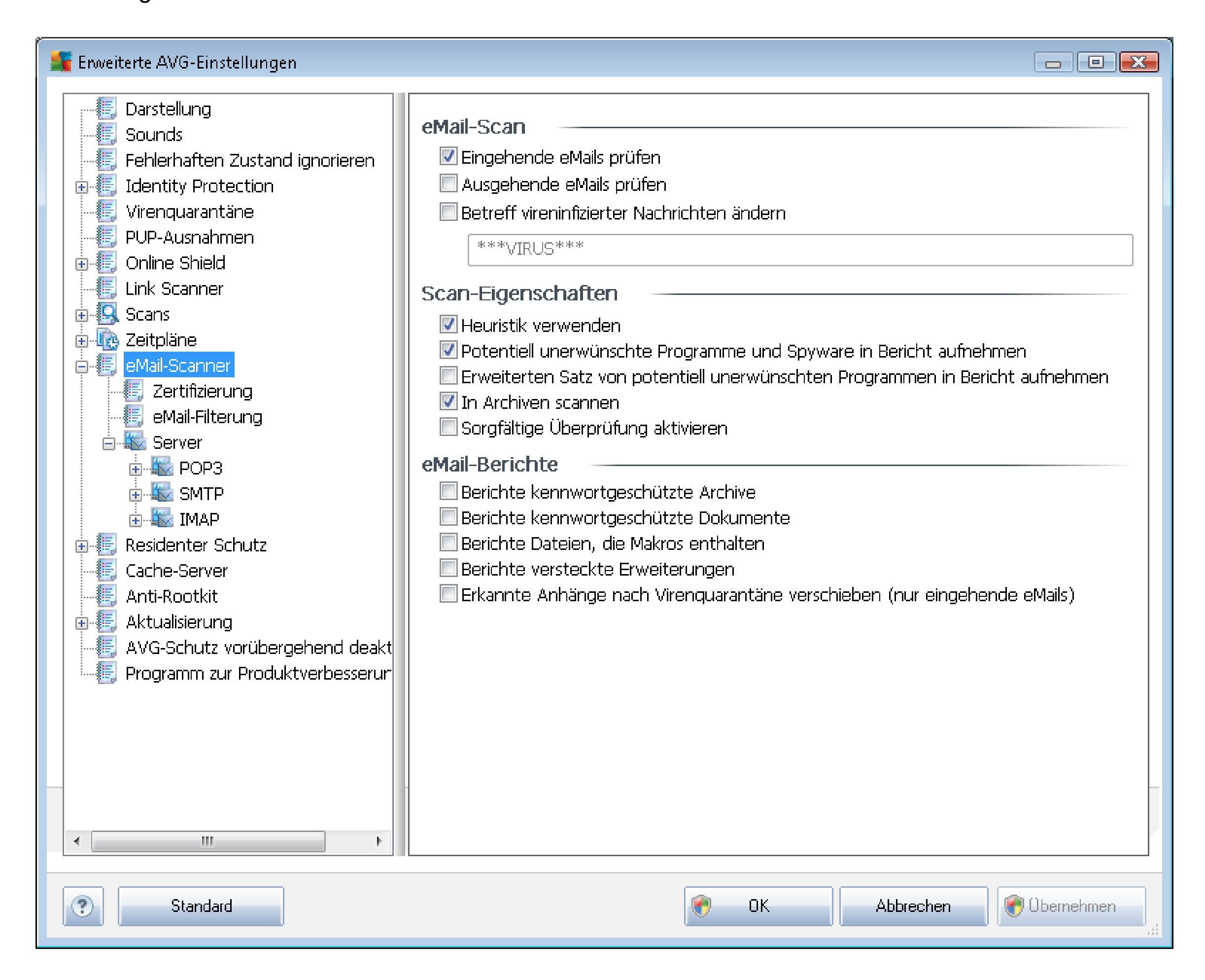
Aktivieren Sie die Option ***Update erneut durchführen, sobald die Internetverbindung aktiv ist***, um sicherzustellen, dass bei einer Unterbrechung der Internetverbindung und dem Fehlschlagen der Aktualisierung das Update unmittelbar nach der Wiederherstellung der Internetverbindung erneut gestartet wird.

Sobald das geplante Update zu der von Ihnen festgelegten Zeit startet, werden Sie darüber in einem Popup-Fenster informiert, das über dem AVG-Symbol im Infobereich geöffnet wird (*vorausgesetzt, Sie haben die Standardeinstellungen im Dialog **Erweiterte Einstellungen/Darstellung** beibehalten*).

Hinweis: *Wenn sich ein geplantes Programm-Update und ein geplanter Scan zeitlich überschneiden, wird der Scan unterbrochen, da das Update eine höhere Priorität hat.*

9.10. eMail-Scanner

Der Dialog ***eMail-Scanner*** ist in drei Bereiche unterteilt:





eMail-Scan

In diesem Abschnitt können Sie folgende Basiseinstellungen für ein- und ausgehende eMail-Nachrichten vornehmen:

- ***Eingehende eMails überprüfen*** (*standardmäßig aktiviert*) – Aktivieren/Deaktivieren Sie diese Option, um alle an Ihren eMail-Client gesendeten Nachrichten zu scannen bzw. nicht zu scannen

- ***Ausgehende eMails überprüfen*** (*standardmäßig deaktiviert*) – Aktivieren/Deaktivieren Sie diese Option, um alle von Ihrem Konto gesendeten eMails zu scannen bzw. nicht zu scannen

- ***Betreff vireninfizierter Nachrichten ändern*** (*standardmäßig deaktiviert*) – Wenn Sie gewarnt werden möchten, dass beim Scannen eine infizierte eMail erkannt wurde, aktivieren Sie diesen Eintrag, und geben Sie im Textfeld den gewünschten Text ein. Dieser Text wird dem Betreff jeder infizierten eMail-Nachricht hinzugefügt , um die Identifikation und Filterung zu erleichtern. Der Standardtext lautet ***VIRUS***. Wir empfehlen, diesen beizubehalten.

Scan-Eigenschaften

In diesem Abschnitt können Sie festlegen, wie die eMail-Nachrichten gescannt werden sollen:

- ***Heuristik verwenden*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, um als Erkennungsmethode beim Scannen der eMail-Nachrichten die Heuristik zu verwenden. Wenn diese Option aktiviert ist, werden eMail-Anhänge nicht nur anhand ihrer Dateierweiterungen gefiltert. Der eigentliche Inhalt des Anhangs wird ebenfalls betrachtet. Die Filterung kann im Dialog ***eMail-Filterung*** eingestellt werden.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***In Archiven scannen*** (*standardmäßig aktiviert*) – Aktivieren Sie diese Option, um den Inhalt von Archiven zu scannen, die an eMail-Nachrichten angehängt sind.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer durch ein Virus oder ein Exploit infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur



Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

Berichte über eMail-Anhänge

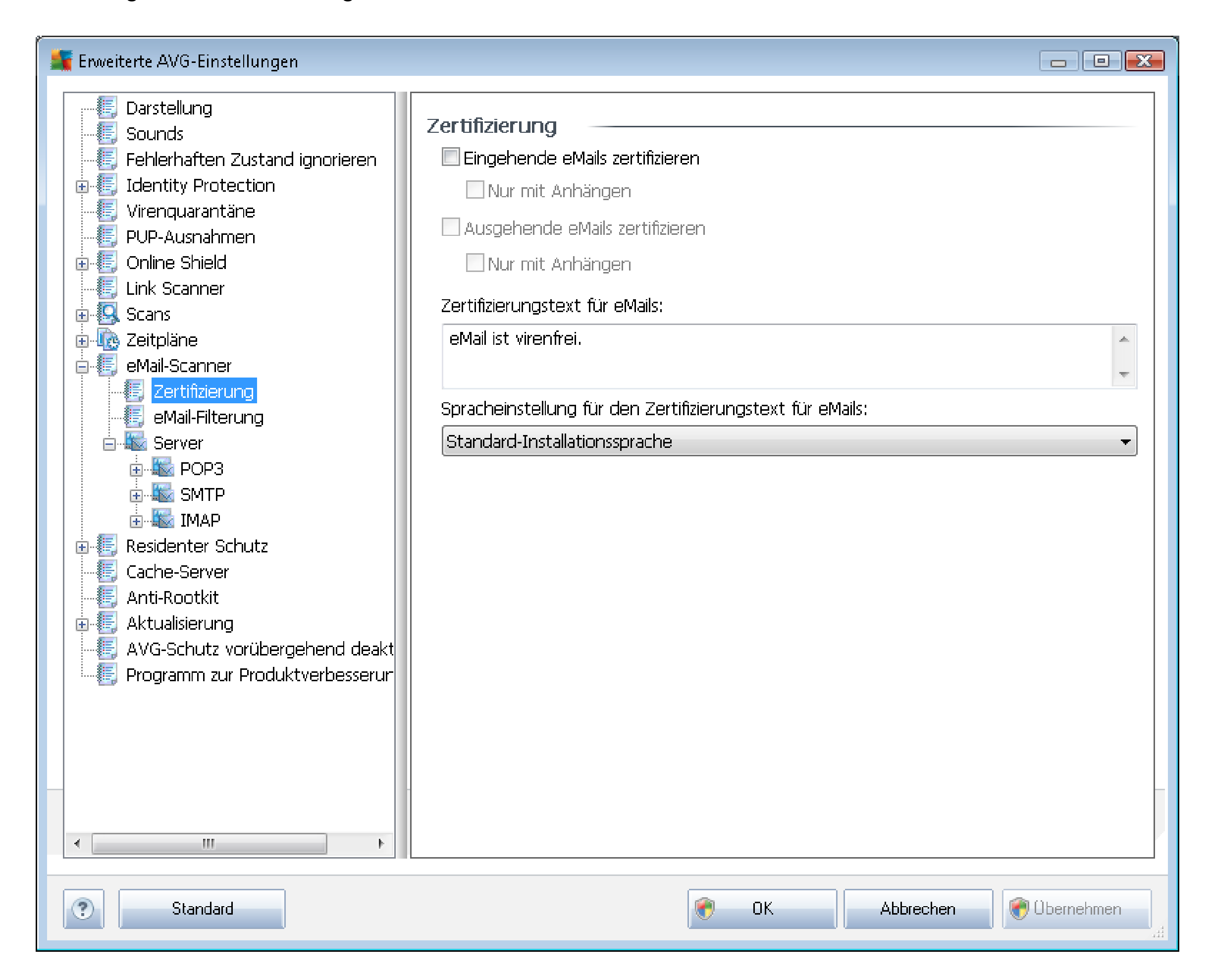
In diesem Bereich können Sie zusätzliche Berichte über Dateien einrichten, die potentiell gefährlich oder verdächtig sein können. Bitte beachten Sie, dass keine Warnung angezeigt wird. Es wird lediglich ein Zertifizierungstext am Ende der eMail-Nachricht angehängt. Alle derartigen Berichte werden im Dialog eMail-Scanner-Erkennung aufgelistet:

- ***Berichte kennwortgeschützte Archive*** – Archive (*ZIP, RAR usw.*) die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Archive als potentiell gefährlich anzuzeigen.
- ***Kennwortgeschützte Dokumente*** – Dokumente, die durch ein Kennwort geschützt sind, können nicht auf Viren gescannt werden. Aktivieren Sie das Kontrollkästchen, um diese Dokumente als potentiell gefährlich anzuzeigen.
- ***Dateien, die Makros enthalten*** – Ein Makro ist eine vordefinierte Abfolge von Schritten, die bestimmte Aufgaben für den Benutzer vereinfachen (*Makros in MS Word sind weitgehend bekannt*). Ein Makro kann z.B. potentiell gefährliche Anweisungen enthalten und durch Aktivieren dieses Kontrollkästchens wird sichergestellt, dass Dateien mit Makros als verdächtig eingestuft werden.
- ***Berichte versteckte Erweiterungen*** – Durch versteckte Erweiterungen kann beispielsweise eine verdächtige ausführbare Datei wie „abcdef.txt.exe“ als eine harmlose Textdatei „abcdef.txt“ angezeigt werden. Aktivieren Sie das Kontrollkästchen, um diese Dateien als potentiell gefährlich anzuzeigen.
- ***Erkannte Anhänge in die Virenquarantäne verschieben*** – Geben Sie an, ob Sie per eMail über kennwortgeschützte Archive, kennwortgeschützte Dokumente, Dateien mit Makros und/oder Dateien mit versteckter Erweiterung benachrichtigt werden möchten, die als Anhang der gescannten eMail-Nachricht erkannt wurden. Wird eine solche Nachricht während des Scans identifiziert, geben Sie an, ob das erkannte infektiöse Objekt in die ***Virenquarantäne*** verschoben werden soll.



9.10.1. Zertifizierung

Im Dialog ***Zertifizierung*** können Sie den Text und die Sprache von Zertifizierungen für eingehende und ausgehende eMails angeben:



Der Text für die Zertifizierung setzt sich aus zwei Teilen zusammen: dem Benutzerteil und dem Systemteil. Im folgenden Beispiel stellt die erste Zeile den Benutzerteil dar, wobei der restliche Text automatisch erstellt wird:

eMail ist virenfrei.

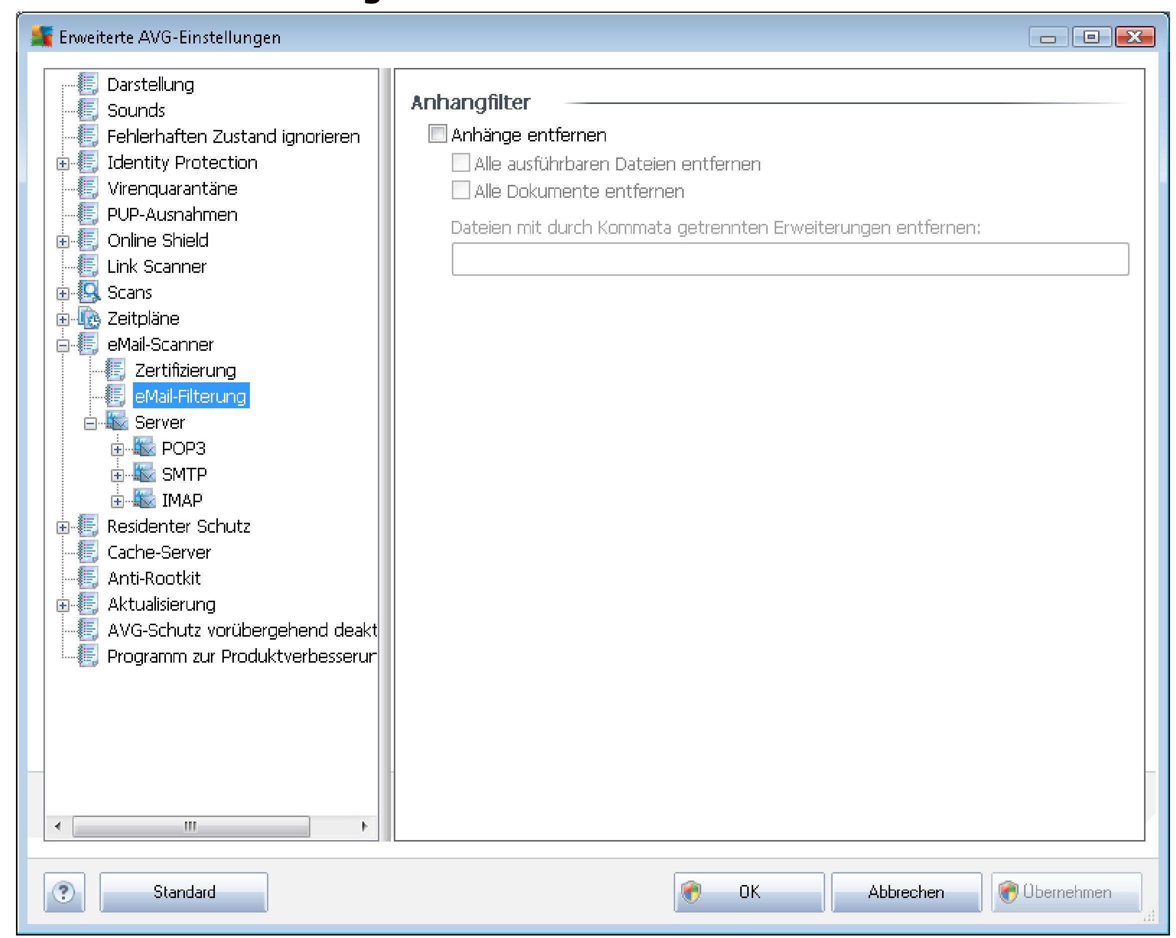
Geprüft von AVG.

Version: x.y.zz / Virendatenbank: xx.y.z – Releasedatum: 12/9/2010

Wenn Sie entweder eingehende oder ausgehende eMails zertifizieren möchten, können Sie in diesem Dialog den Zertifizierungstext des Benutzerteils festlegen (***Zertifizierungstext für eMails:***) und auswählen, in welcher Sprache der automatisch erstellte Systemteil des Zertifizierungstexts angezeigt werden soll (***Spracheinstellung für den Zertifizierungstext für eMails***).



9.10.2. eMail-Filterung



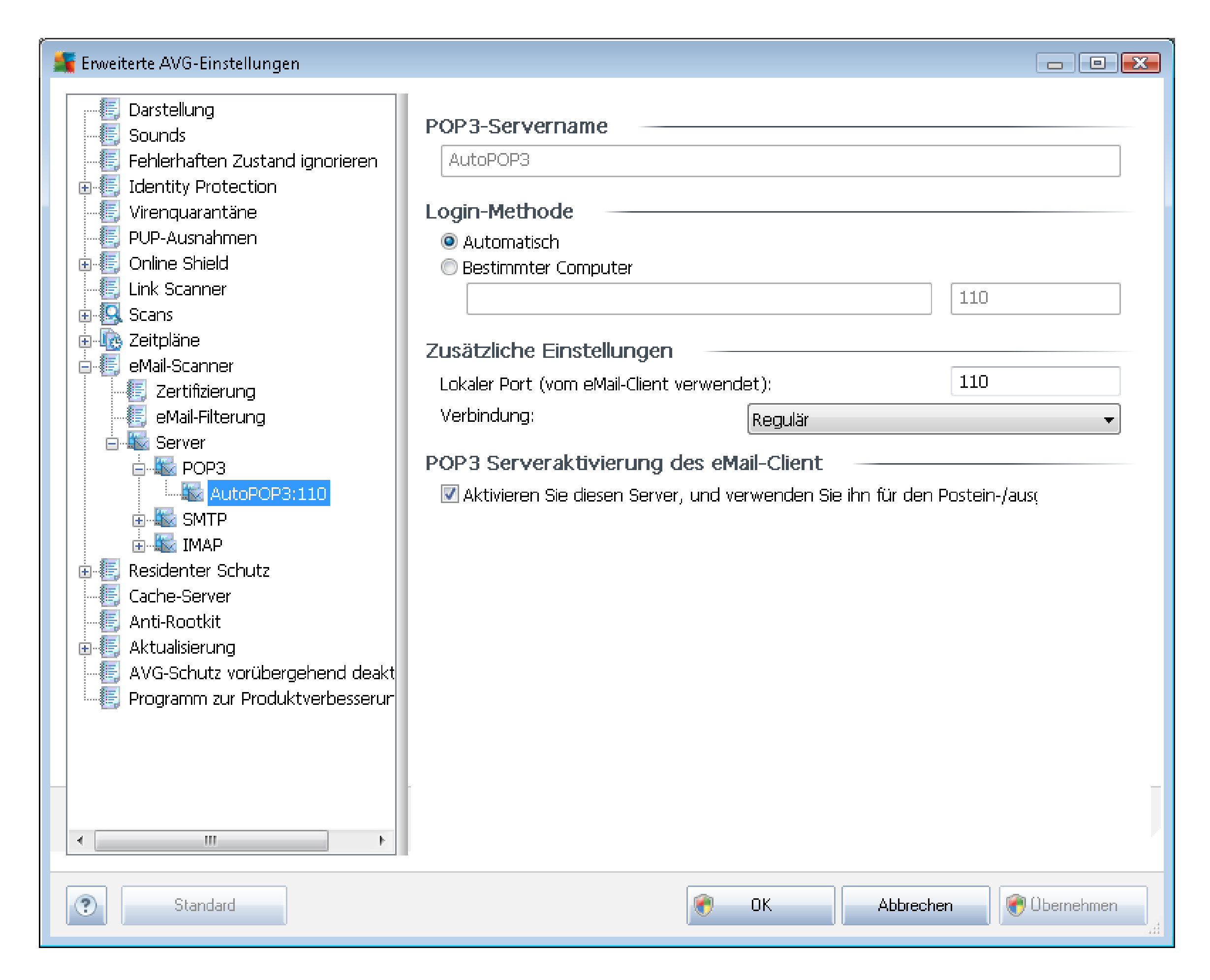
Im Dialog ***Anhangfilter*** können Sie Parameter für das Scannen von eMail-Anhängen festlegen. Standardmäßig ist die Option ***Anhänge entfernen*** deaktiviert. Wenn Sie die Option aktivieren, werden alle eMail-Anhänge, die als infektiös oder potentiell gefährlich erkannt werden, automatisch entfernt. Wenn Sie möchten, dass nur bestimmte Arten von Anhängen entfernt werden, wählen Sie die entsprechende Option aus:

- ***Alle ausführbaren Dateien entfernen*** – Alle Dateien des Typs *.exe werden gelöscht
- ***Alle Dokumente entfernen*** – Alle Dateien mit den folgenden Erweiterungen werden entfernt: *.doc, *.docx, *.xls, *.xlsx
- ***Dateien mit durch Kommata getrennten Erweiterungen entfernen*** – Alle Dateien mit den definierten Erweiterungen werden entfernt

9.10.3. Server

Im Bereich ***Server*** können Sie die Parameter der Server der Komponente ***eMail-Scanner*** bearbeiten oder mit Hilfe der Schaltfläche ***Neuen Server hinzufügen*** einen neuen Server einrichten.





In diesem Dialog (*wird über **Server/POP3*** geöffnet) können Sie einen neuen ***eMail-Scanner***-Server einrichten, der das POP3-Protokoll für eingehende eMails verwenden soll:

- ***POP3-Servername*** – In diesem Feld können sie den Namen des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines POP3-Servers mit der rechten Maustaste auf den POP3-Eintrag im linken Navigationsmenü*). Bei einem automatisch erstellten „AutoPOP3"-Server ist dieses Feld deaktiviert.

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für eingehende eMails bestimmt werden soll:

  - ***Automatisch*** – Die Anmeldung erfolgt den Einstellungen Ihres eMail-Programms entsprechend automatisch.

  - ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres Mailservers an. Der Anmeldename bleibt unverändert. Als Namen können Sie einen Domänennamen (*z. B. pop.acme.com*) oder eine IP-Adresse (*z. B. 123.45.67.89*) verwenden. Wenn der Mailserver keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen



verwendet wird (*z. B. pop.acme.com:8200*). Der Standardport für die POP3-Kommunikation ist 110.

- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:
    - o ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung ankommen soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die POP3-Kommunikation angeben.
    - o ***Verbindung*** – In diesem Dropdown-Menü können Sie angeben, welche Verbindungsart verwendet werden soll (*regulär/SSL/SSL-Standardwert*). Wenn Sie die SSL-Verbindung wählen, werden die Daten verschlüsselt versendet, und es besteht kein Risiko, dass sie von Dritten verfolgt oder überwacht werden. Diese Funktion steht ebenfalls nur dann zur Verfügung, wenn der Ziel-Mailserver sie unterstützt.
- ***Serveraktivierung für eMail-Client POP3*** – Markieren Sie diese Option, um den angegebenen POP3-Server zu aktivieren oder zu deaktivieren

Erweiterte AVG-Einstellungen

Darstellung
Sounds
Fehlerhaften Zustand ignorieren
Identity Protection
Virenquarantäne
PUP-Ausnahmen
Online Shield
Link Scanner
Scans
Zeitpläne
eMail-Scanner
Zertifizierung
eMail-Filterung
Server
POP3
SMTP
AutoSMTP:25
IMAP
Residenter Schutz
Cache-Server
Anti-Rootkit
Aktualisierung
AVG-Schutz vorübergehend deakt
Programm zur Produktverbesserur

SMTP-Servername
AutoSMTP
Login-Methode
Automatisch
Bestimmter Computer
25
Zusätzliche Einstellungen
Lokaler Port (vom eMail-Client verwendet): 25
Verbindung: Regulär
SMTP Serveraktivierung des eMail-Client
Aktivieren Sie diesen Server, und verwenden Sie ihn für den Postein-/ausg

Standard
OK
Abbrechen
Übernehmen

In diesem Dialog (*wird über **Server/SMTP*** geöffnet) können Sie einen neuen ***eMail-Scanner***-Server einrichten, der das SMTP-Protokoll für ausgehende eMails verwendet:



- ***SMTP-Servername*** – In diesem Feld können sie den Name des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines SMTP-Servers mit der rechten Maustaste auf den SMTP-Eintrag im linken Navigationsmenü*). Bei einem automatisch erstellten „AutoSMTP"-Server ist dieses Feld deaktiviert.

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für ausgehende eMails bestimmt werden soll:

  - ***Automatisch*** – Die Anmeldung erfolgt automatisch, den Einstellungen Ihres eMail-Programms entsprechend

  - ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres eMail-Servers an. Als Namen können Sie einen Domainnamen (*z. B. smtp.acme.com*) oder eine IP-Adresse (*z. B. 123.45.67.89*) verwenden. Wenn der Mailserver keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen verwendet wird (*z. B. smtp.acme.com:8200*). Der Standardport für die SMTP-Kommunikation ist 25.

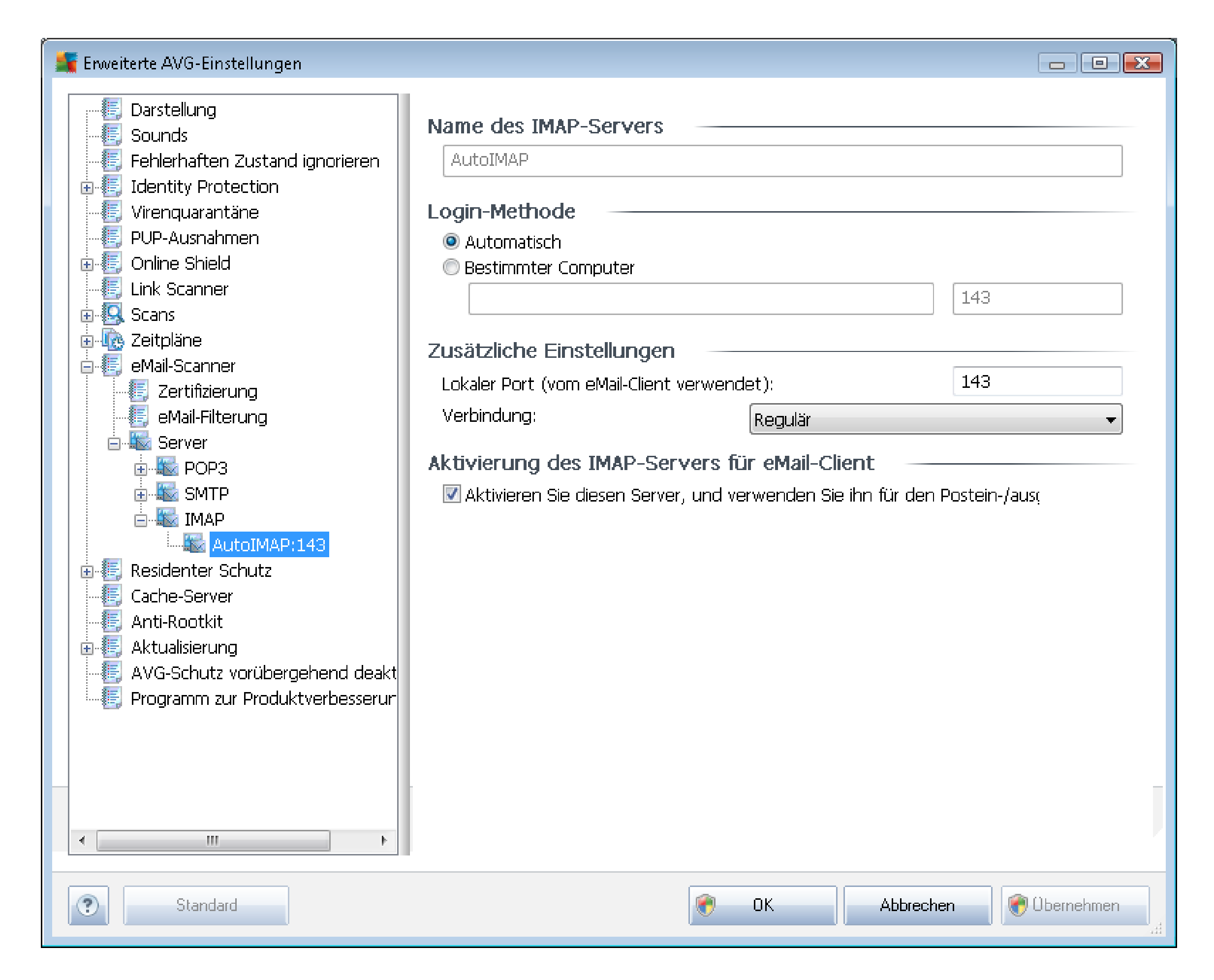
- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:

  - ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung ankommen soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die SMTP-Kommunikation angeben.

  - ***Verbindung*** – In diesem Dropdown-Menü können Sie angeben, welche Verbindungsart verwendet werden soll (*regulär/SSL/SSL-Standardwert*). Wenn Sie die SSL-Verbindung wählen, werden die Daten verschlüsselt versendet, und es besteht kein Risiko, dass sie von Dritten verfolgt oder überwacht werden. Diese Funktion steht nur dann zur Verfügung, wenn der Ziel-eMail-Server sie unterstützt.

- ***SMTP-Serveraktivierung des eMail-Client*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten SMTP-Server zu aktivieren/deaktivieren





In diesem Dialog (wird über ***Server/IMAP*** geöffnet) können Sie einen neuen ***eMail-Scanner***-Server einrichten, der das IMAP-Protokoll für ausgehende eMails verwendet:

- ***IMAP-Servername*** – In diesem Feld können sie den Name des neu hinzugefügten Servers angeben (*Klicken Sie zum Hinzufügen eines IMAP-Servers mit der rechten Maustaste auf den IMAP-Eintrag im linken Navigationsmenü*). Bei einem automatisch erstellten „AutoIMAP"-Server ist dieses Feld deaktiviert.

- ***Login-Methode*** – Legen Sie fest, mit welcher Methode der Mailserver für ausgehende eMails bestimmt werden soll:

  - ***Automatisch*** – Die Anmeldung erfolgt automatisch, den Einstellungen Ihres eMail-Programms entsprechend

  - ***Bestimmter Computer*** – In diesem Fall verwendet das Programm immer den hier angegebenen Server. Geben Sie bitte die Adresse oder den Namen Ihres eMail-Servers an. Als Namen können Sie einen Domainnamen (*z. B. imap.acme.com*) oder eine IP-Adresse (*z. B. 123.45.67.89*) verwenden. Wenn der eMail-Server keinen Standardport verwendet, können Sie den Port hinter dem Servernamen angeben, wobei ein Doppelpunkt als Trennzeichen verwendet wird (*z. B. imap.acme.com:8200*

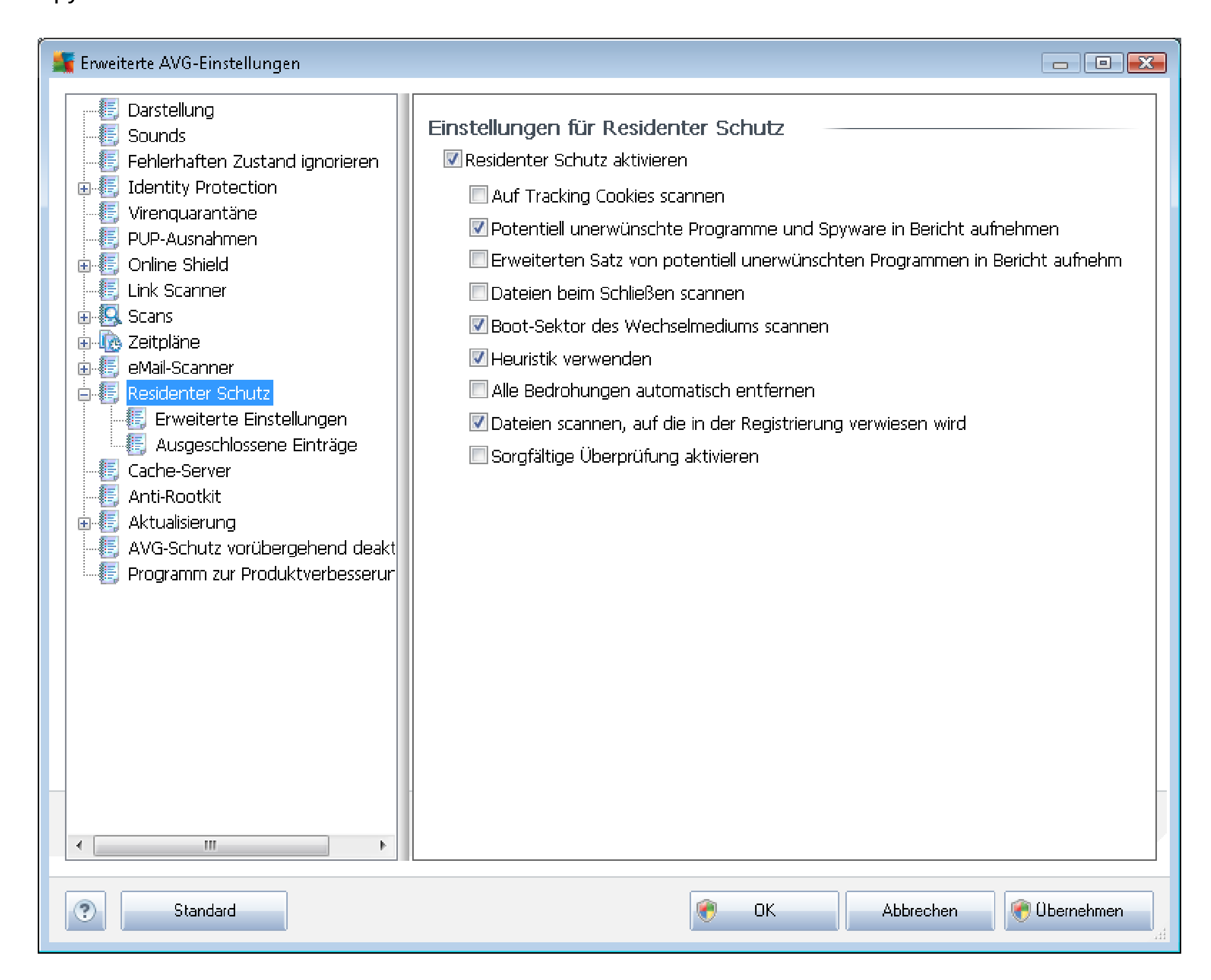


). Der Standardport für die IMAP-Kommunikation ist 143.

- ***Zusätzliche Einstellungen*** – Hier werden Parameter detaillierter festgelegt:
  - ***Lokaler Port*** – Hiermit wird der Port festgelegt, auf dem die Kommunikation von Ihrer eMail-Anwendung ankommen soll. In Ihrem eMail-Programm müssen Sie diesen Port als Port für die IMAP-Kommunikation angeben.
  - ***Verbindung*** – In diesem Dropdown-Menü können Sie angeben, welche Verbindungsart verwendet werden soll (*regulär/SSL/SSL-Standardwert*). Wenn Sie die SSL-Verbindung wählen, werden die Daten verschlüsselt versendet, und es besteht kein Risiko, dass sie von Dritten verfolgt oder überwacht werden. Diese Funktion steht nur dann zur Verfügung, wenn der Ziel-eMail-Server sie unterstützt.
- ***IMAP-Serveraktivierung des eMail-Clients*** – Aktivieren/Deaktivieren Sie dieses Kontrollkästchen, um den zuvor festgelegten IMAP-Server zu aktivieren/deaktivieren

9.11. Residenter Schutz

Die Komponente ***Residenter Schutz*** bietet Echtzeitschutz von Dateien und Ordnern gegen Viren, Spyware und andere Malware.





Im Dialog ***Einstellungen für Residenter Schutz*** können Sie den Schutz durch ***Residenter Schutz*** vollständig aktivieren oder deaktivieren, indem Sie die Option ***Residenter Schutz aktivieren*** aktivieren oder deaktivieren (*Standardmäßig ist diese Option aktiviert*). Darüber hinaus können Sie auswählen, welche Features von ***Residenter Schutz*** aktiviert werden sollen:

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Mit diesem Parameter wird festgelegt, dass während des Scanvorgangs Cookies erkannt werden sollen. (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*)

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** – (*standardmäßig aktiviert*): Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Dateien beim Schließen scannen*** (*standardmäßig deaktiviert*) – Diese Option sorgt dafür, dass AVG aktive Objekte (z. B. Anwendungen oder Dokumente) sowohl beim Öffnen als auch beim Beenden scannt. Durch dieses Feature ist Ihr Computer auch vor einigen fortschrittlichen Virenarten geschützt

- ***Boot-Sektor des Wechselmediums scannen*** (*standardmäßig aktiviert*)

- ***Heuristik verwenden*** – (*standardmäßig aktiviert*) Die heuristische Analyse wird zum Erkennen verwendet (*dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*)

- ***Alle Bedrohungen automatisch entfernen*** (*standardmäßig deaktiviert*) – Jede erkannte Infektion wird automatisch geheilt, wenn eine Gegenmaßnahme verfügbar ist. Infektionen, die nicht geheilt werden können, werden entfernt.

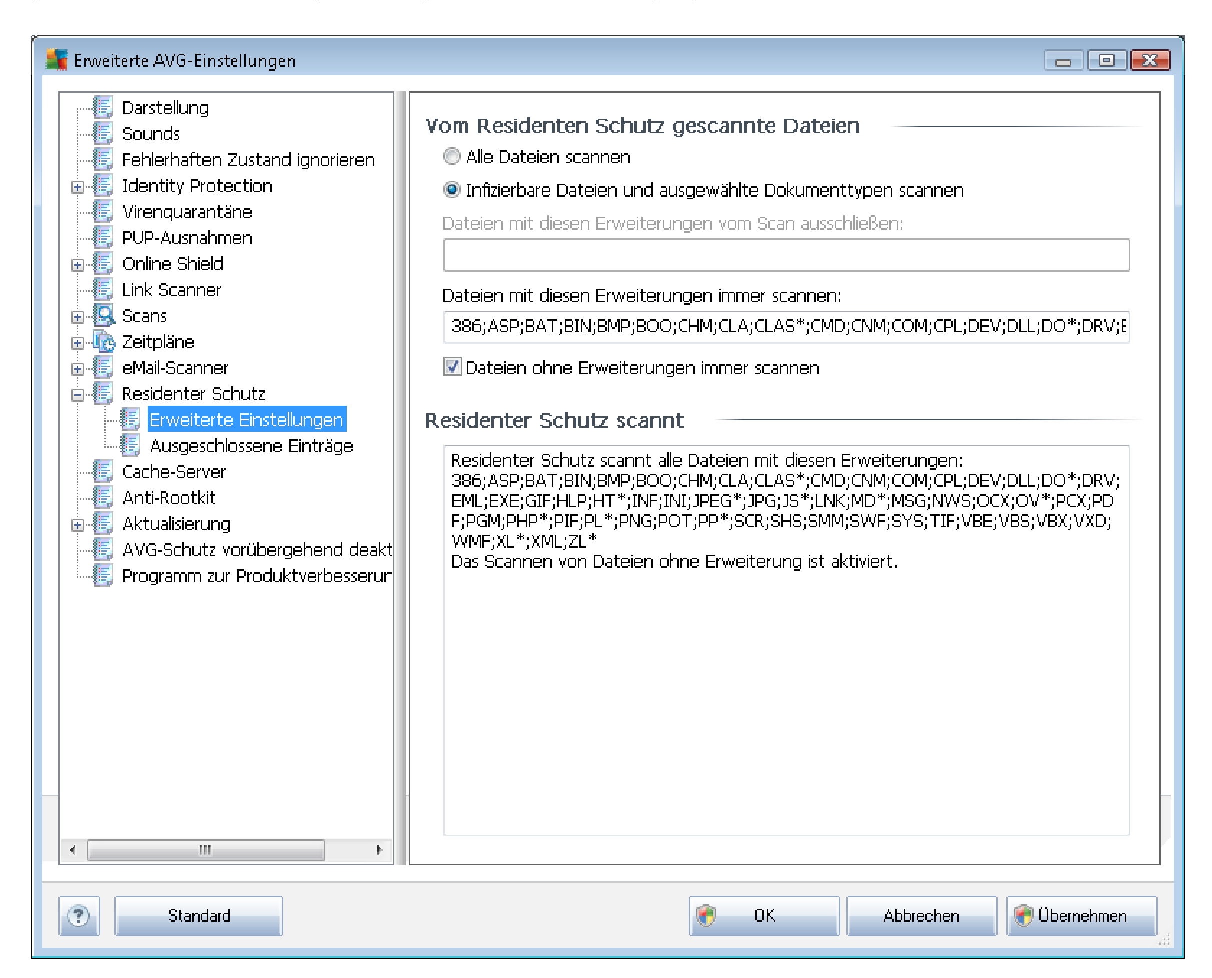
- ***Dateien scannen, auf die in der Registrierung verwiesen wird*** (*standardmäßig aktiviert*) – Mit diesem Parameter wird festgelegt, dass AVG alle ausführbaren Dateien der Startup-Registrierung scannt, um zu verhindern, dass eine bekannte Infektion beim nächsten Computerstart ausgeführt wird.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*in extremen Notfällen*), um einen sorgfältigen Scan zu starten, bei dem alle möglichen, bedrohlichen Objekte genauestens überprüft werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.



9.11.1. Erweiterte Einstellungen

Im Dialog ***Vom Residenten Schutz gescannte Dateien*** können Sie festlegen, welche Dateien gescannt werden sollen (*durch Angabe der Erweiterungen*):

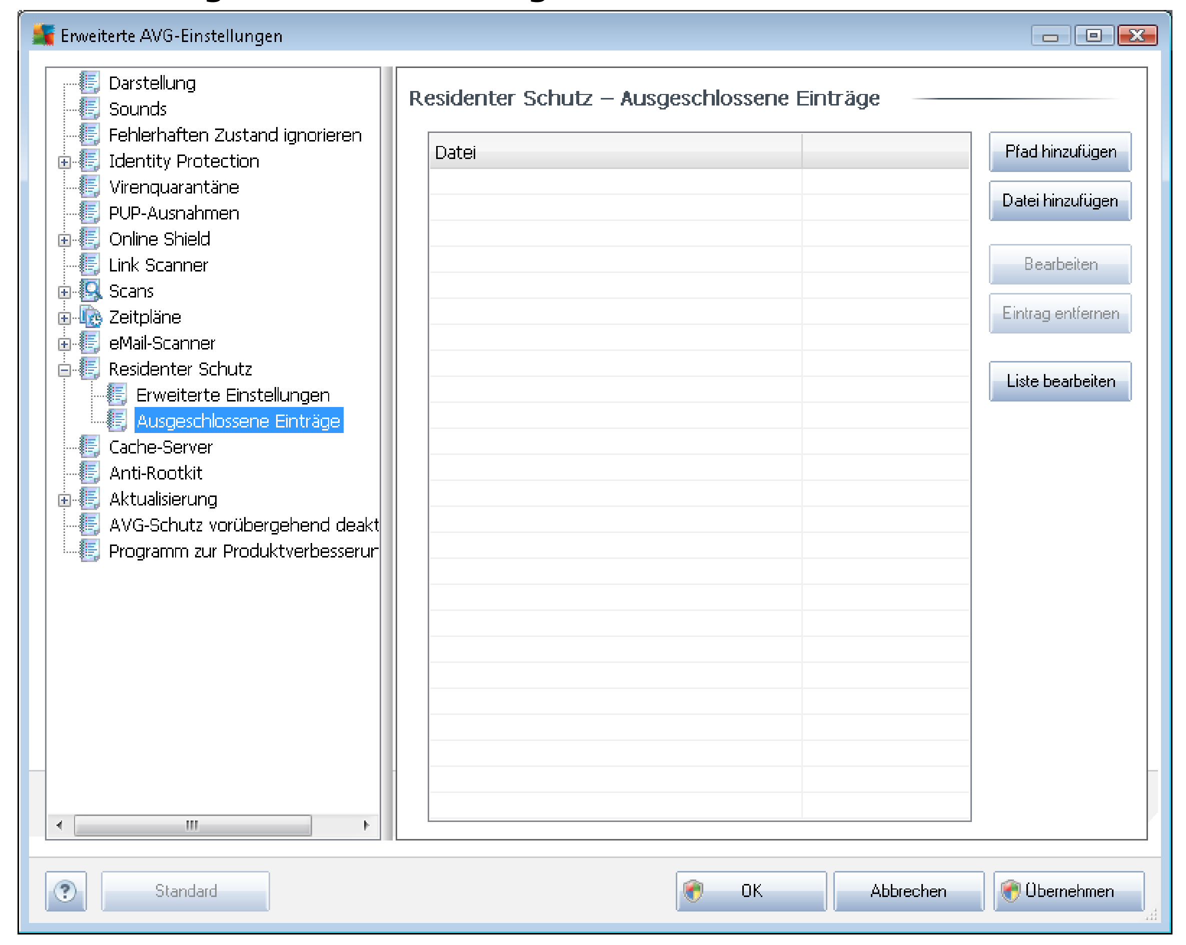


Sie können festlegen, ob alle Dateien oder nur infizierbare Dateien gescannt werden sollen. Im letzteren Fall können Sie zwei Listen von Erweiterungen angeben, um zu bestimmen, welche Dateitypen vom Scan ausgeschlossen werden sollen und welche Dateitypen in jedem Fall gescannt werden sollen.

Im unteren Bereich ***Residenter Schutz scannt*** werden die aktuellen Einstellungen zusammengefasst und detailliert angezeigt, was vom ***Residenten Schutz*** tatsächlich gescannt wird.



9.11.2. Ausgeschlossene Einträge



Im Dialog ***Residenter Schutz – Ausgeschlossene Einträge*** können Sie Dateien und/oder Ordner definieren, die von der Überprüfung durch den ***Residenten Schutz*** ausgeschlossen werden sollen.

Wenn dies nicht unbedingt notwendig ist, empfehlen wir dringend, keine Einträge auszuschließen!

Der Dialog enthält folgende Schaltflächen:

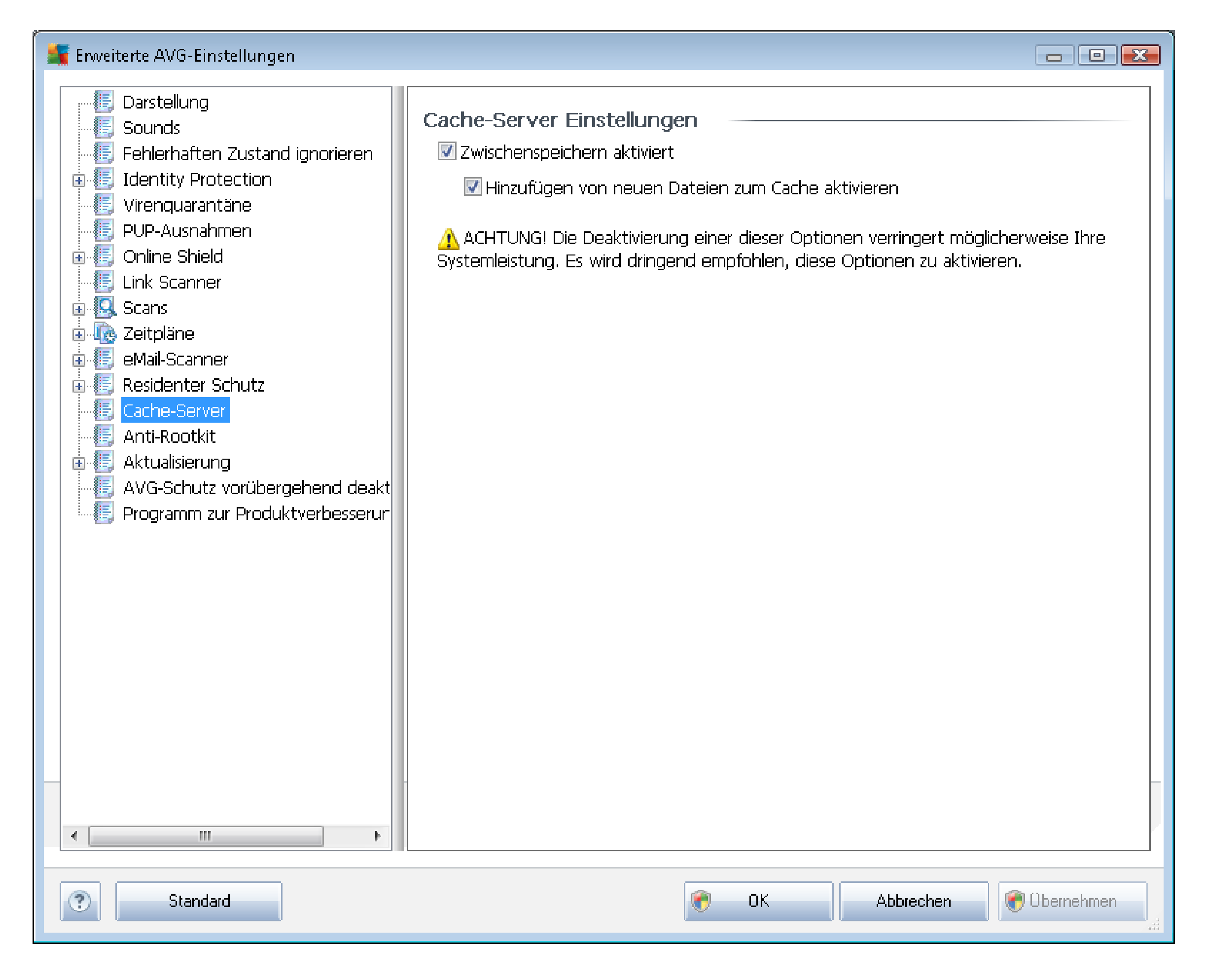
- ***Pfad hinzufügen*** – Mit dieser Schaltfläche können Sie ein oder mehrere Verzeichnisse angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Datei hinzufügen*** – Mit dieser Schaltfläche können Sie Dateien angeben, die vom Scan ausgeschlossen werden sollen, indem Sie diese einzeln aus der Baumstruktur der lokalen Festplatte auswählen
- ***Bearbeiten*** – Hier können Sie den festgelegten Pfad zu einer ausgewählten Datei oder einem ausgewählten Ordner bearbeiten
- ***Eintrag entfernen***– Mit dieser Schaltfläche können Sie den Pfad zu einem ausgewählten



Eintrag aus der Liste löschen

9.12. Cache-Server

Der ***Cache-Server*** ist ein Prozess, der alle Scans (*On-Demand-Scan, geplanter Scan des gesamten Computers, Scan durch den [Residenten Schutz]*) beschleunigen soll. Er sammelt und speichert Informationen vertrauenswürdiger Dateien (*Systemdateien mit digitaler Signatur usw.*): Diese Dateien werden als sicher eingestuft und beim Scan übersprungen.



Im Dialog „Einstellungen“ stehen zwei Optionen zur Verfügung:

- ***Zwischenspeichern aktiviert*** (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, um den ***Cache-Server*** zu deaktivieren und den Zwischenspeicher zu leeren. Beachten Sie, dass Scans möglicherweise langsamer ablaufen und die Gesamtleistung des Computers beeinträchtigt wird, da jede einzelne verwendete Datei zunächst auf Viren und Spyware gescannt wird.

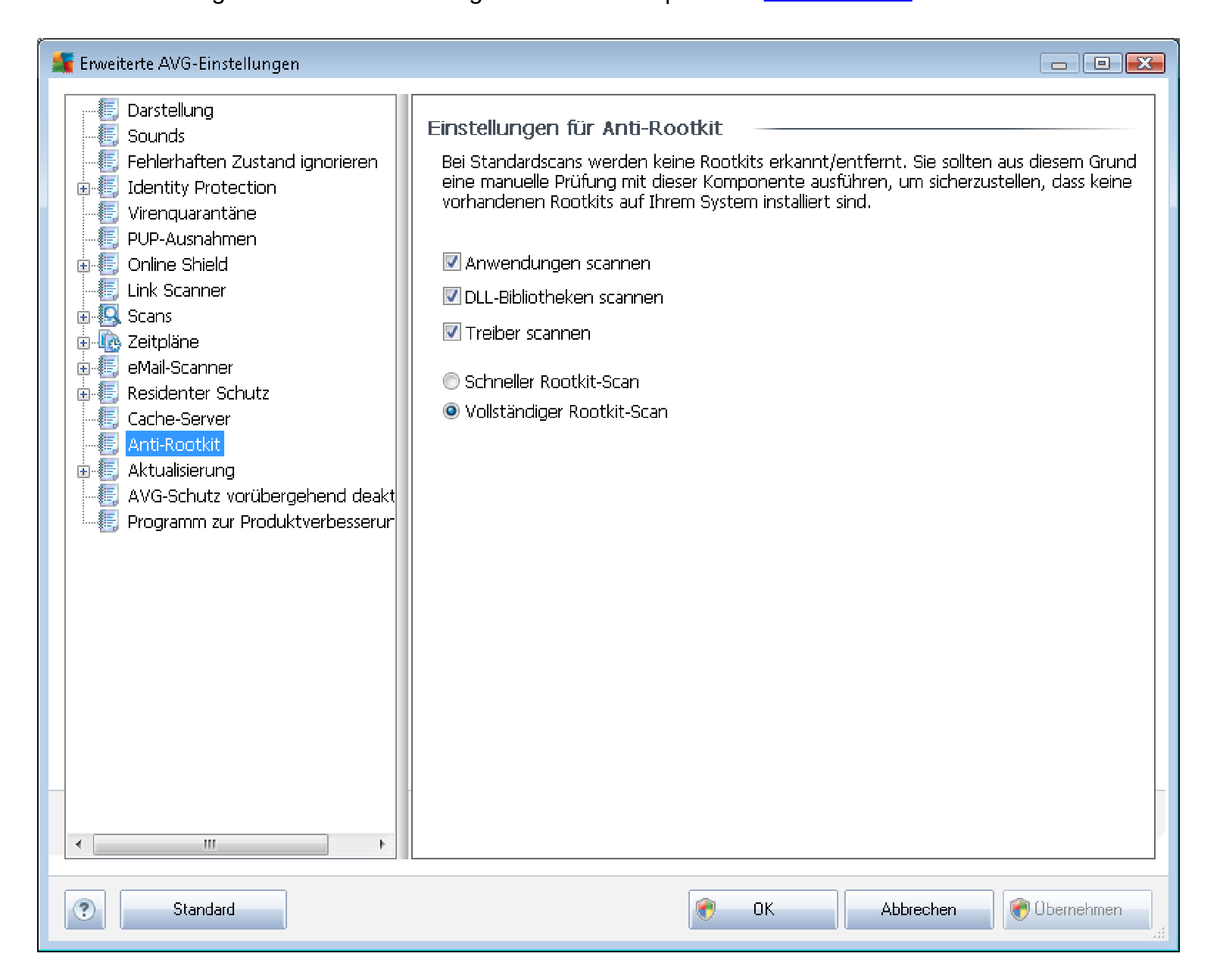
- ***Hinzufügen von neuen Dateien zum Cache aktivieren*** (*standardmäßig aktiviert*) – Deaktivieren Sie dieses Kontrollkästchen, und dem Zwischenspeicher werden keine weiteren Dateien hinzugefügt. Dateien, die sich bereits im Zwischenspeicher befinden, bleiben darin enthalten und werden bis zum nächsten Update der Virendatenbank oder bis



zum vollständigen Ausschalten des Zwischenspeichers weiter verwendet.

9.13. Anti-Rootkit

In diesem Dialog können Sie die Konfiguration der Komponente ***Anti-Rootkit*** bearbeiten:



Die Bearbeitung aller Funktionen der Komponente ***Anti-Rootkit*** kann auch direkt über die ***Benutzeroberfläche der Komponente Anti-Rootkit*** vorgenommen werden.

Aktivieren Sie die entsprechenden Kontrollkästchen, um festzulegen, welche Objekte gescannt werden sollen:

- ***Anwendungen scannen***
- ***DLL-Bibliotheken scannen***
- ***Treiber scannen***

Wählen Sie anschließend den Rootkit-Scanmodus aus:

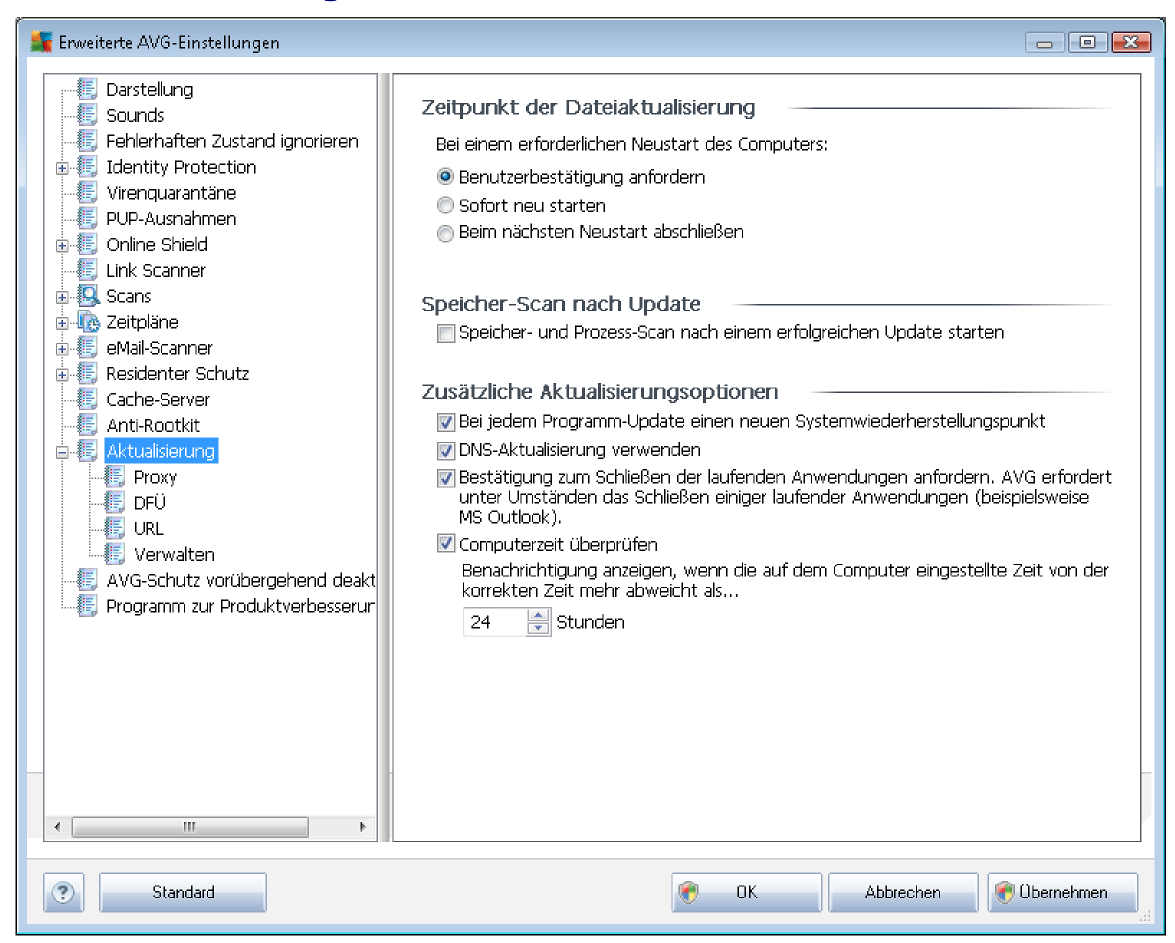
- ***Schneller Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber und den



Systemordner (*typischerweise C:\WINDOWS*)

- ***Vollständiger Rootkit-Scan*** – prüft alle laufenden Prozesse, geladenen Treiber, den Systemordner (*typischerweise C:\WINDOWS*) und zusätzlich alle lokalen Festplatten (*einschließlich Flash-Disks, aber keine Disketten-/CD-Laufwerke*)

9.14. Aktualisierung



Mit dem Navigationselement ***Update*** wird ein neuer Dialog geöffnet, in dem Sie allgemeine Parameter hinsichtlich der Aktualisierung von AVG festlegen können:

Zeitpunkt der Dateiaktualisierung

In diesem Bereich können Sie zwischen drei alternativen Optionen wählen, wenn der Update-Vorgang einen Neustart des Computers erfordert. Der Abschluss des Updates kann für den nächsten Neustart des Computers geplant werden, oder Sie können den Neustart sofort durchführen:

- ***Benutzerbestätigung anfordern*** *(standardmäßig)* – Sie werden aufgefordert, den Neustart Ihres Computers zu bestätigen, um den Updatevorgang abzuschließen



- ***Sofort neu starten*** – der Computer wird automatisch neu gestartet, unmittelbar nachdem der Updatevorgang abgeschlossen ist. Sie müssen den Neustart nicht bestätigen

- ***Beim nächsten Neustart abschließen*** – der Abschluss des Updatevorgangs wird bis zum nächsten Neustart des Computers verschoben. Bitte beachten Sie, dass diese Option nur empfohlen wird, wenn Sie sicher sind, dass der Computer regelmäßig – mindestens einmal täglich – neu gestartet wird!

Speicher-Scan nach Update

Aktivieren Sie dieses Kontrollkästchen, um nach jedem erfolgreich abgeschlossenen Update einen Scan des Speichers durchzuführen. Das zuletzt heruntergeladene Update kann neue Virendefinitionen enthalten, die beim Scanvorgang umgehend angewendet werden.

Zusätzliche Aktualisierungsoptionen

- ***Bei jedem Programmupdate einen neuen Systemwiederherstellungspunkt erstellen*** – Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen Konfiguration wiederherstellen. Diese Option kann über Start/Programme/Zubehör/Systemprogramme/ Systemwiederherstellung aufgerufen werden. Änderungen sollten jedoch nur von erfahrenen Benutzern vorgenommen werden! Wenn Sie diese Funktion nutzen möchten, lassen Sie dieses Kontrollkästchen aktiviert.

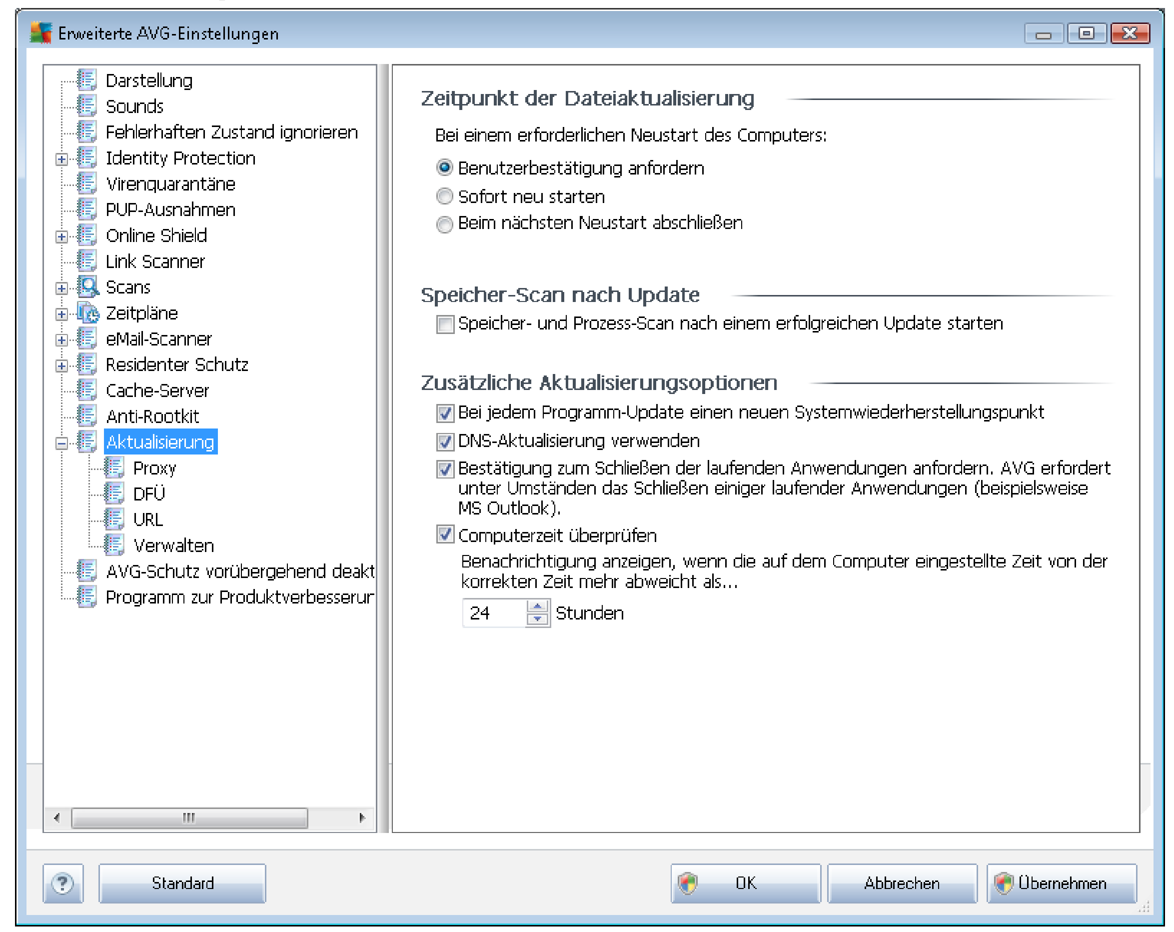
- ***DNS-Update verwenden*** (*Standard*) – Ist diese Option aktiviert, sucht Ihr **AVG Anti-Virus 2011** die Informationen der neuesten Version der Virendatenbank auf dem DNS-Server, sobald das Update gestartet wird. Dann werden nur die kleinsten unabdingbar erforderlichen Aktualisierungsdateien heruntergeladen und ausgeführt. Auf diese Weise wird die heruntergeladene Datenmenge auf einem Minimum gehalten und der Aktualisierungsprozess ist schneller.

- ***Mithilfe der Option „Bestätigung zum Schließen der laufenden Anwendungen anfordern“*** (*standardmäßig aktiviert*) können Sie dafür sorgen, dass keine aktuell ausgeführten Anwendungen ohne Ihre Genehmigung geschlossen werden. Dies kann zum Abschluss des Updatevorgangs erforderlich sein;

- ***Computerzeit überprüfen*** – Aktivieren Sie diese Option, wenn eine Benachrichtigung angezeigt werden soll, falls die Computerzeit um mehr als die angegebene Anzahl an Stunden von der korrekten Zeit abweicht.



9.14.1. Proxy



Ein Proxy-Server ist ein unabhängiger Server oder Dienst, der auf einem PC ausgeführt wird und für eine sicherere Verbindung mit dem Internet sorgt. Sie können auf das Internet entsprechend den festgelegten Netzwerkregeln entweder direkt oder über den Proxy-Server zugreifen. Es können auch beide Möglichkeiten gleichzeitig zugelassen sein. Wählen Sie anschließend im Dialog ***Aktualisierungseinstellungen – Proxy*** aus dem Dropdown-Menü eine der folgenden Optionen aus:

- ***Proxy verwenden***
- ***Keinen Proxy verwenden*** – Standardeinstellungen
- ***Stellen Sie eine direkte Verbindung her, wenn eine Proxy-Verbindung fehlschägt***

Wenn Sie eine Option mit Proxy-Server ausgewählt haben, müssen Sie weitere Angaben machen. Die Servereinstellungen können entweder manuell oder automatisch vorgenommen werden.

Manuelle Konfiguration

Wenn Sie die manuelle Konfiguration auswählen (aktivieren Sie *die Option* ***Manuell*** *, um den*



jeweiligen Dialog zu aktivieren), müssen Sie folgende Angaben machen:

- ***Server*** – Geben Sie die IP-Adresse oder den Namen des Servers an
- ***Port*** – Geben Sie die Portnummer für den Internetzugriff an (*Standardmäßig ist die Portnummer 3128 zugewiesen. Sie können diese aber ändern. Wenn Sie sich nicht sicher sind, wenden Sie sich an Ihren Netzwerkadministrator*)

Auf dem Proxy-Server können auch besondere Regeln für jeden Benutzer festgelegt sein. Aktivieren Sie in diesem Fall das Kontrollkästchen ***PROXY-Authentifizierung verwenden***, um zu bestätigen, dass Ihr Benutzername und Ihr Kennwort für die Verbindung mit dem Internet über den Proxy-Server gültig sind.

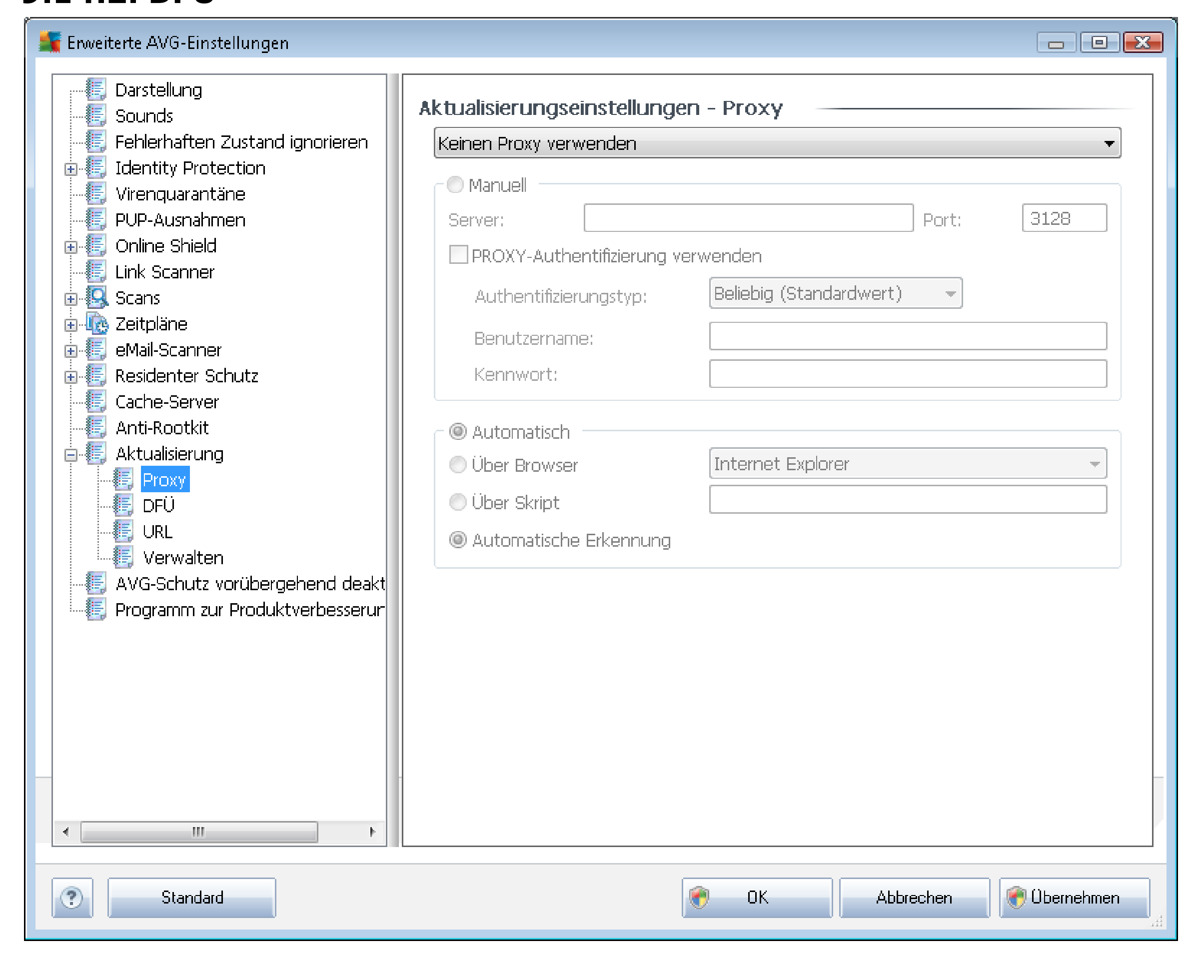
Automatische Konfiguration

Wenn Sie die automatische Konfiguration auswählen (*Aktivieren Sie die Option **Automatisch**, um den Dialog zu aktivieren*), wählen Sie bitte aus, von wo die Konfiguration des Proxy vorgenommen werden soll:

- ***Über Browser*** – Die Konfiguration wird von Ihrem Standard-Internetbrowsers gelesen
- ***Über Skript*** – Die Konfiguration wird von einem heruntergeladenen Skript gelesen, das die Proxy-Adresse wiedergibt
- ***Automatische Erkennung*** – Die Konfiguration wird automatisch direkt vom Proxy-Server erkannt



9.14.2. DFÜ

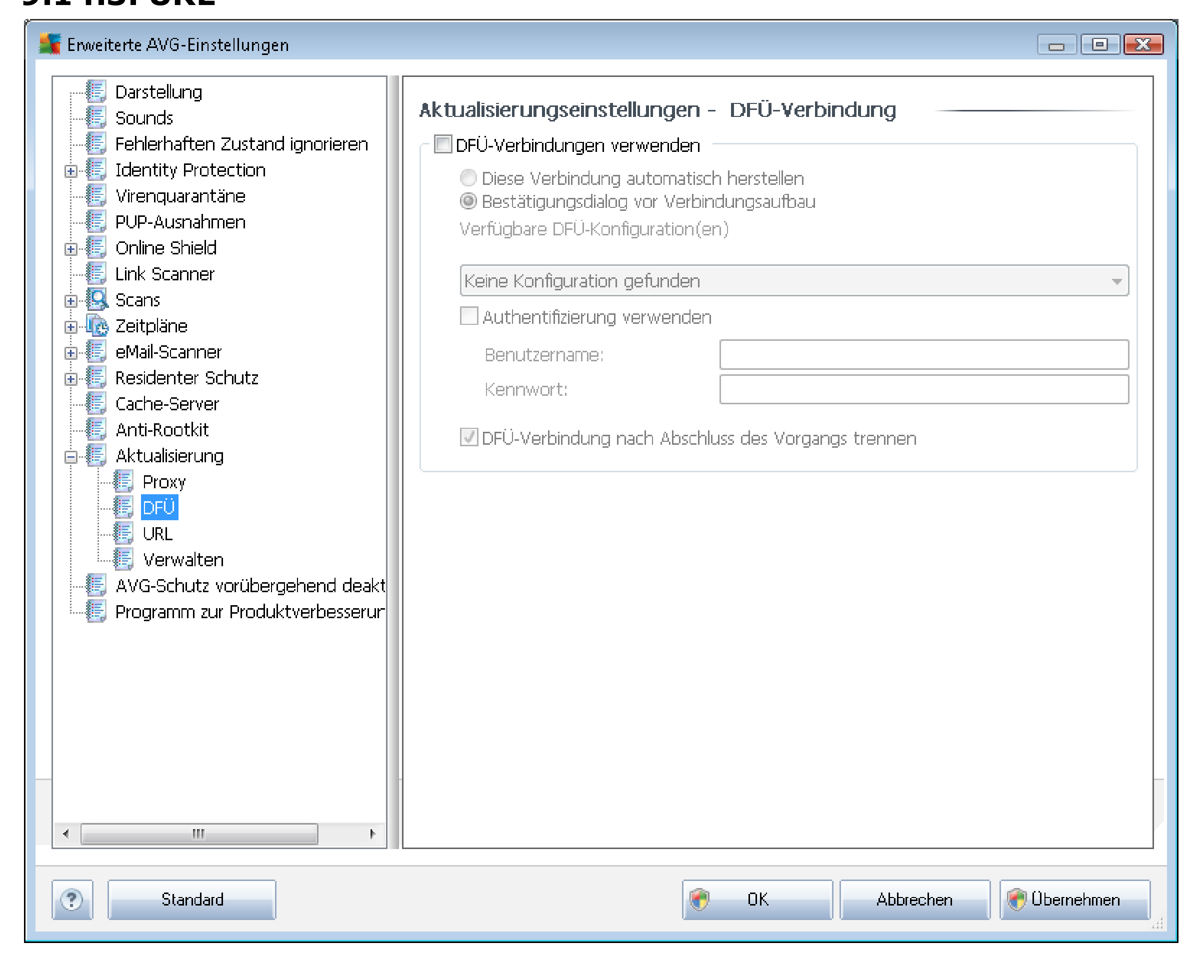


Die optional im Dialog ***Aktualisierungseinstellungen – DFÜ-Verbindung*** definierten Parameter beziehen sich auf die Einwahlverbindung mit dem Internet. Die Felder des Dialogs werden erst aktiviert, wenn Sie die Option ***DFÜ-Verbindungen verwenden*** auswählen.

Geben Sie an, ob die Verbindung mit dem Internet automatisch hergestellt werden soll (***Diese Verbindung automatisch herstellen***) oder ob Sie die Verbindung jedes Mal bestätigen möchten (***Bestätigungsdialog vor Verbindungsaufbau***). Bei der automatischen Verbindungsherstellung sollten Sie zudem auswählen, ob die Verbindung nach Abschluss der Aktualisierung getrennt werden soll (***DFÜ-Verbindung nach Abschluss des Vorgangs trennen***).



9.14.3. URL



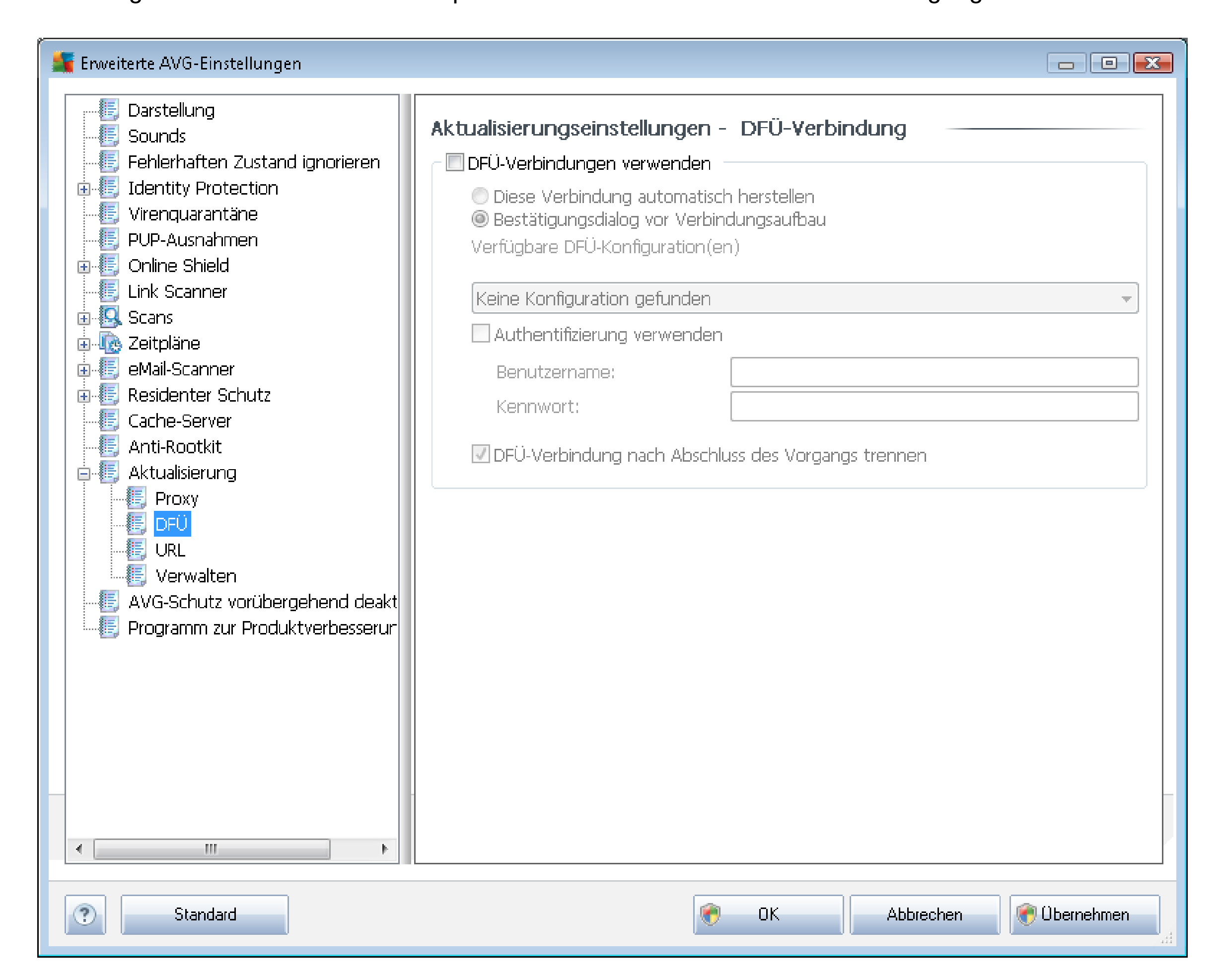
Der Dialog ***URL*** zeigt eine Liste von Internetadressen an, von denen Updates heruntergeladen werden können. Die Liste kann über die folgenden Schaltflächen geändert werden:

- ***Hinzufügen*** – Ein Dialog wird geöffnet, in dem Sie der Liste eine neue URL hinzufügen können
- ***Bearbeiten*** – Ein Dialog wird geöffnet, in dem Sie die Parameter der ausgewählten URL bearbeiten können
- ***Löschen*** – Die ausgewählte URL wird aus der Liste gelöscht
- ***Nach oben*** – Die ausgewählte URL wird in der Liste eine Position nach oben verschoben
- ***Nach unten*** – Die ausgewählte URL-Adresse wird in der Liste eine Position nach unten verschoben



9.14.4. Verwalten

Im Dialog ***Verwalten*** stehen zwei Optionen über zwei Schaltflächen zur Verfügung:

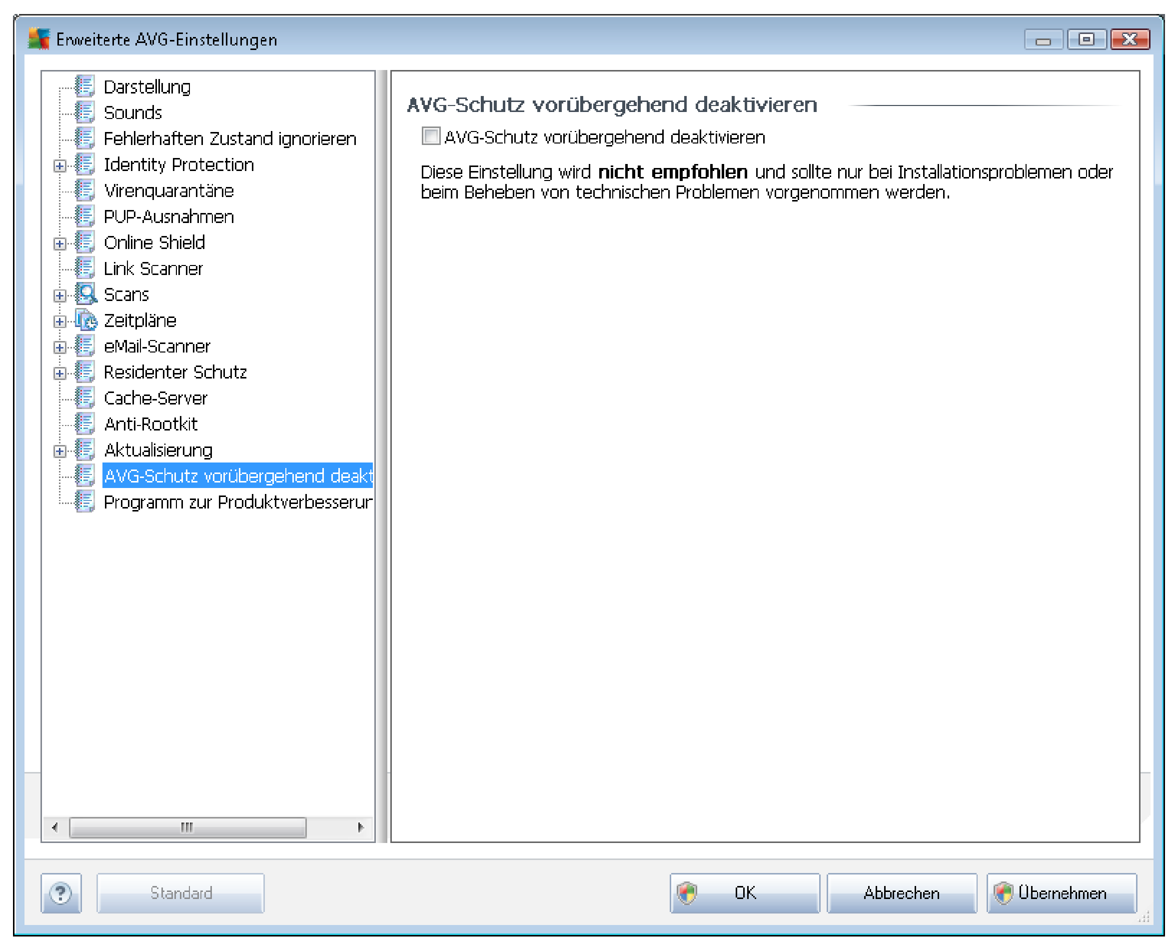


- ***Temporäre Aktualisierungsdateien löschen*** – Klicken Sie auf diese Schaltfläche, wenn Sie alle redundanten Update-Dateien von Ihrer Festplatte löschen möchten (*standardmäßig werden diese Dateien 30 Tage gespeichert*)

- ***Virendatenbank auf vorhergehende Version zurücksetzen*** – Klicken Sie auf diese Schaltfläche, um die letzte Version der Virendatenbank auf Ihrer Festplatte zu löschen und zur vor diesem Update gespeicherten Version zurückzukehren (*Die neue Version der Virendatenbank ist Teil des nächsten Update*)



9.15. AVG-Schutz vorübergehend deaktivieren



Im Dialog ***AVG-Schutz vorübergehend deaktivieren*** können Sie alle Schutzfunktionen von **AVG Anti-Virus 2011** gleichzeitig deaktivieren.

Verwenden Sie diese Option nur, wenn es unbedingt erforderlich ist.

In der Regel ***müssen Sie AVG nicht deaktivieren***, bevor Sie neue Software oder Treiber installieren , auch wenn das Installationsprogramm oder der Software-Assistent darauf hinweist, dass laufende Programme und Anwendungen beendet werden müssen, um den Installationsvorgang ohne Unterbrechungen abzuschließen. Wenn Sie während der Installation jedoch ein Problem feststellen, deaktivieren Sie zunächst die Komponente ***Residenter Schutz***. Wenn Sie AVG vorübergehend deaktivieren müssen, denken Sie daran, es so bald wie möglich wieder zu aktiveren. Ihr Computer ist Bedrohungen ausgesetzt, wenn Sie bei deaktivierter Virenschutz-Software mit dem Internet oder einem Netzwerk verbunden sind.

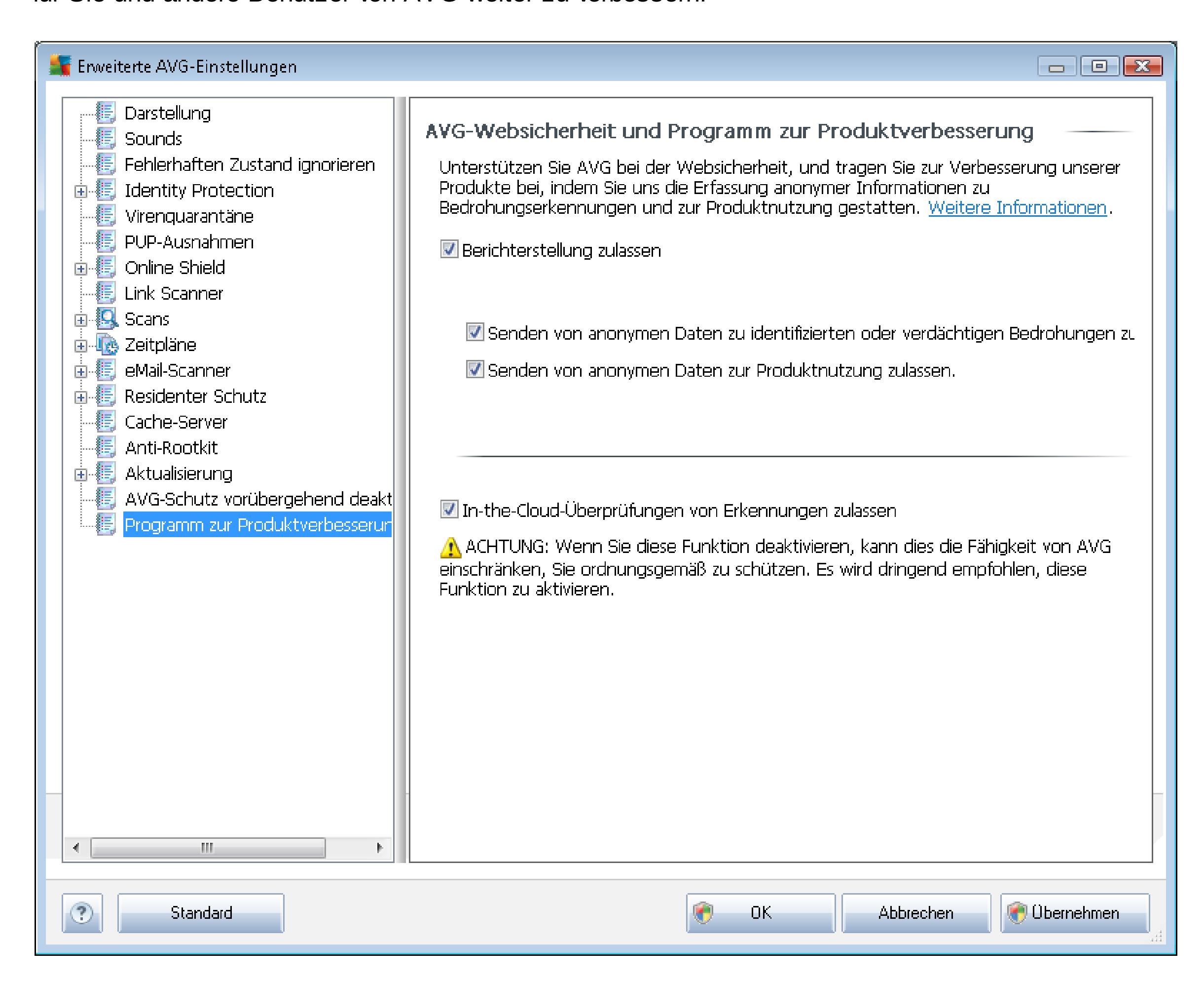
9.16. Programm zur Produktverbesserung

Der Dialog ***AVG-Websicherheit und Programm zur Produktverbesserung*** lädt Sie zur Teilnahme an der AVG-Produktverbesserung ein, wodurch Sie uns bei der Verbesserung der allgemeinen Internetsicherheit unterstützen. Aktivieren Sie die Option ***Berichterstellung zulassen***, um die



Berichterstattung über erkannte Bedrohungen an AVG zu aktivieren. Auf diese Weise erhalten wir aktuelle Informationen über Bedrohungen von allen Benutzern auf der ganzen Welt und können im Gegenzug unseren Schutz für alle noch weiter verbessern.

Die Berichterstattung erfolgt automatisch und ohne Beeinträchtigungen; in den Berichten sind keine persönlichen Daten enthalten. Die Berichterstellung über erkannte Bedrohungen ist optional. Wir möchten Sie jedoch bitten, diese Funktion ebenfalls zu aktivieren, da sie uns hilft, den Schutz für Sie und andere Benutzer von AVG weiter zu verbessern.



Es gibt heutzutage weit mehr Bedrohungen als reine Viren. Urheber von schädlichen Codes und gefährlichen Websites zeigen sich stets einfallsreich, und neue Bedrohungen tauchen immer wieder auf, die meisten davon im Internet. Im Folgenden werden einige der häufigsten beschrieben:

- ***Ein Virus ist ein schädlicher Code, der sich selbst vervielfältigt und sich ohne Erlaubnis und Wissen der Benutzer auf Computern verbreitet und Schäden anrichtet.*** Einige Viren stellen ernstere Bedrohungen dar, da sie Dateien löschen oder manipulieren können; andere Viren hingegen sind eher harmlos und spielen beispielsweise nur eine Musikdatei ab. Unabhängig von der Gefährlichkeit können alle Viren jedoch aufgrund ihrer Fähigkeit zur Vervielfältigung rasch den gesamten Speicher in Beschlag nehmen und den Computer zum Absturz bringen.



- ***Würmer*** sind eine Unterkategorie von Viren, die jedoch kein Trägerobjekt zur Verbreitung benötigen, sie verbreiten sich ohne Zutun des Benutzers. In aller Regel geschieht dies per eMail, und es kommt zu Überlastungen von eMail-Servern und Netzwerksystemen.

- ***Spyware*** ist eine Malware-Kategorie (*Malware = jede schädliche Software, einschließlich Viren*), eingebunden in Programme (üblicherweise Trojaner), die persönliche Informationen, Kennwörter, Kreditkartennummern stehlen oder in einen Computer eindringen und es dem Angreifer ermöglichen, die Kontrolle über den Computer zu übernehmen, natürlich ohne das Wissen oder die Einwilligung des Computerbesitzers.

- ***Potentiell unerwünschte Programme*** sind eine Art Spyware, die eine Gefahr für Ihren Computer darstellen können, aber nicht müssen. Ein typisches Beispiel für ein PUP ist Adware, eine Software zur Verteilung von Werbung, die meist in störenden Popup-Fenstern angezeigt wird, aber keinen Schaden anrichten.

- Αυχη ***Tracking Cookies*** sind eine Art Spyware, da diese kleinen Dateien im Webbrowser gespeichert werden und automatisch an eine Stamm-Website gesendet werden, wenn diese Seite noch einmal besucht wird. Sie enthalten dann Daten wie das Surfverhalten und andere ähnlicher Informationen.

- ***Exploit*** ist ein gefährlicher Code, der Schlupflöcher oder Schwachstellen im Betriebssystem, Internetbrowser oder in anderen wichtigen Programmen ausnutzt.

- Μιτ ***Phishing*** bezeichnet man den Versuch, an sensible persönliche Daten heranzukommen, indem vorgetäuscht wird, dass es sich um eine vertrauenswürdige und bekannte Organisation handelt. Normalerweise werden die potentiellen Opfer über eine Massen-eMail gebeten, z. B. die Zugangsdaten zu ihrem Bankkonto zu aktualisieren. Sie sollen dazu dem angegebenen Link folgen, der sie dann auf eine gefälschte Website der Bank führt.

- ***Hoax bezeichnet eine Massen-eMail, die gefährliche, alarmierende oder einfach belästigende und nutzlose Informationen enthält.*** Viele der oben genannten Bedrohungen verwenden Hoax-eMails als Verbreitungsmethode.

- ***Verseuchte Websites*** sind Websites, durch die gefährliche Software auf Ihrem Computer installiert wird, sowie infizierte Seiten, die dasselbe tun, wobei es sich in diesem Fall um legitime Websites handelt, die beschädigt wurden und dazu benutzt werden, Besucher zu infizieren.

Um Sie vor diesen verschiedenen Bedrohungen zu schützen, bietet AVG folgende besonderen Komponenten:

- ***Anti-Virus***, um Ihren Computer vor Viren zu schützen,

- ***Anti-Spyware***, um Ihren Computer vor Spyware zu schützen,

- ***Online Shield***, um Sie beim Surfen im Internet vor Viren und Spyware zu schützen,

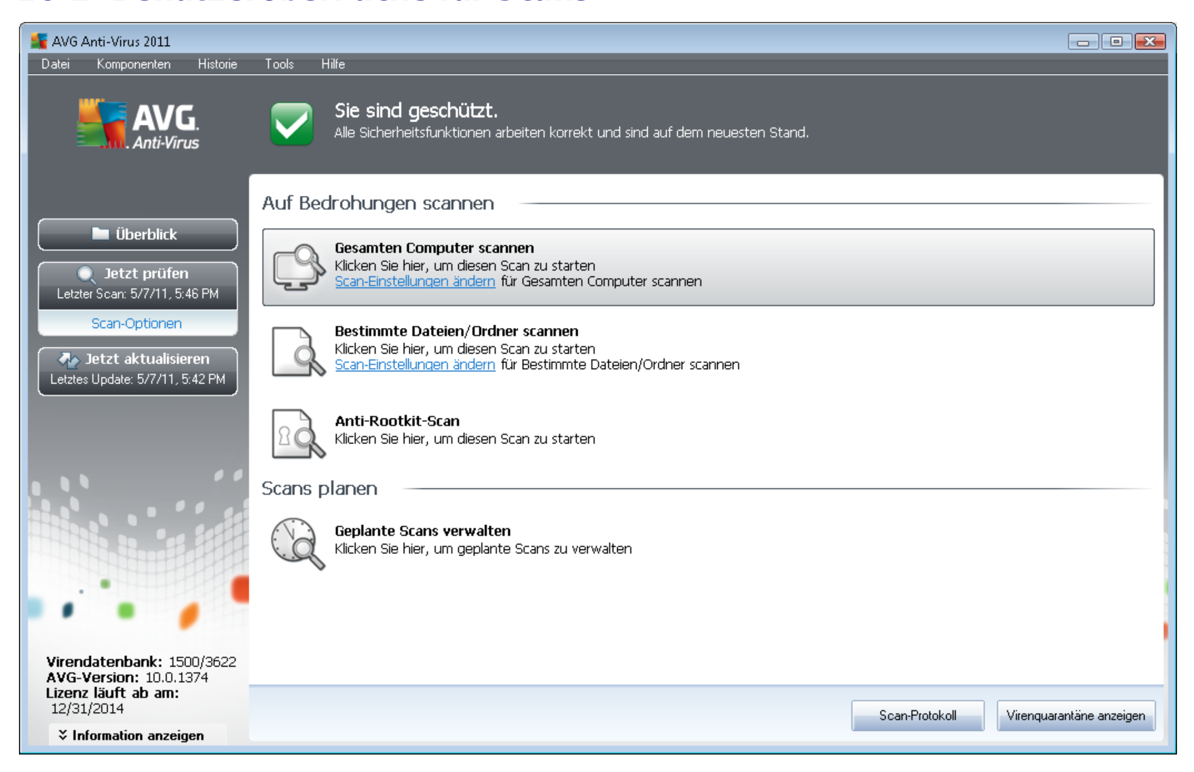
- ***Link Scanner***, um Sie vor anderen in diesem Kapitel beschriebenen Online-Bedrohungen zu schützen.



10. AVG-Scans

Die Durchführung von Scans ist eine der wichtigsten Funktionen von **AVG Anti-Virus 2011**. Sie können Scans nach Bedarf (on-Demand) ausführen oder geplant regelmäßig nach einem festgelegten Zeitplan, der Ihren Anforderungen entspricht.

10.1. Benutzeroberfläche für Scans



Auf die Benutzeroberfläche für Scans von AVG kann über den Quick Link***Scan-Optionen*** zugegriffen werden. Klicken Sie auf den Link, um zum Dialog ***Auf Bedrohungen scannen*** zu wechseln. Im Dialog finden Sie Folgendes:

- Übersicht über vordefinierte Scans – Drei verschiedene vom Softwarehersteller definierte Scans, die sich On-Demand oder in Zeitplänen verwenden lassen:
    - o ***Gesamten Computer scannen***
    - o ***Bestimmte Dateien/Ordner scannen***
    - o ***Anti-Rootkit-Scan***
- Bereich Einstellungen für geplanten Scan" – Hier können Sie gegebenenfalls neue Scans definieren und neue Zeitpläne erstellen.

Schaltflächen



Auf der Scan-Oberfläche stehen Ihnen folgende Schaltflächen zur Verfügung:

- ***Scan-Protokoll*** – Hiermit wird der Dialog ***Übersicht über Scan-Ergebnisse*** mit dem gesamten Protokoll der Scans angezeigt
- ***Virenquarantäne anzeigen*** – Hiermit wird ein neues Fenster mit der ***Virenquarantäne*** geöffnet – ein Bereich, in dem erkannte Infektionen unter Quarantäne gestellt werden

10.2. Vordefinierte Scans

Eine der Hauptfunktionen von**AVG Anti-Virus 2011** ist der On-Demand-Scan. Tests On-Demand wurden entwickelt, um verschiedene Teile eines Computers zu scannen, wenn der Verdacht einer Virusinfektion besteht. Es wird dringend empfohlen, derartige Tests regelmäßig durchzuführen, auch wenn Sie denken, dass sich auf dem Computer kein Virus befinden kann.

In **AVG Anti-Virus 2011** stehen die folgenden vom Software-Hersteller vordefinierten Arten von Scans zur Verfügung:

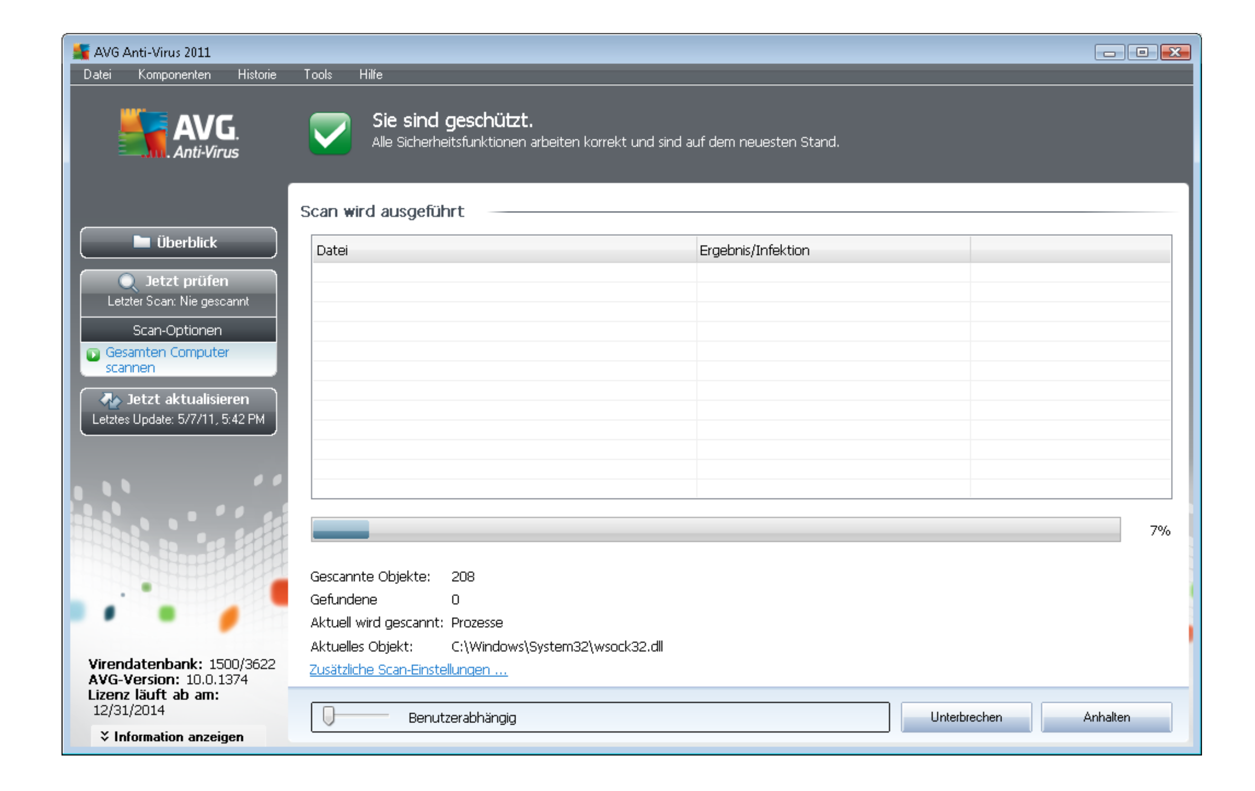
10.2.1. Scan des gesamten Computers

Scan des gesamten Computers – Hiermit wird Ihr gesamter Computer nach möglichen Infektionen und/oder potentiell unerwünschten Programmen gescannt. Bei diesem Scan werden alle Festplatten Ihres Computers gescannt, gefundene Viren werden geheilt oder erkannte Infektionen in die ***Virenquarantäne*** verschoben. Ein Scan des gesamten Computers sollte auf einer Workstation mindestens einmal pro Woche geplant werden.

Start von Scans

Sie können den ***Scan des gesamten Computers*** direkt über die Benutzeroberfläche für Scans starten, indem Sie auf das Scan-Symbol klicken. Für diesen Scan-Typ müssen keine weiteren Einstellungen vorgenommen werden. Der Scan startet sofort im Dialog ***Scan wird ausgeführt*** (*siehe Screenshot*). Der Scanvorgang kann bei Bedarf unterbrochen (***Unterbrechen***) oder abgebrochen (***Anhalten***) werden.

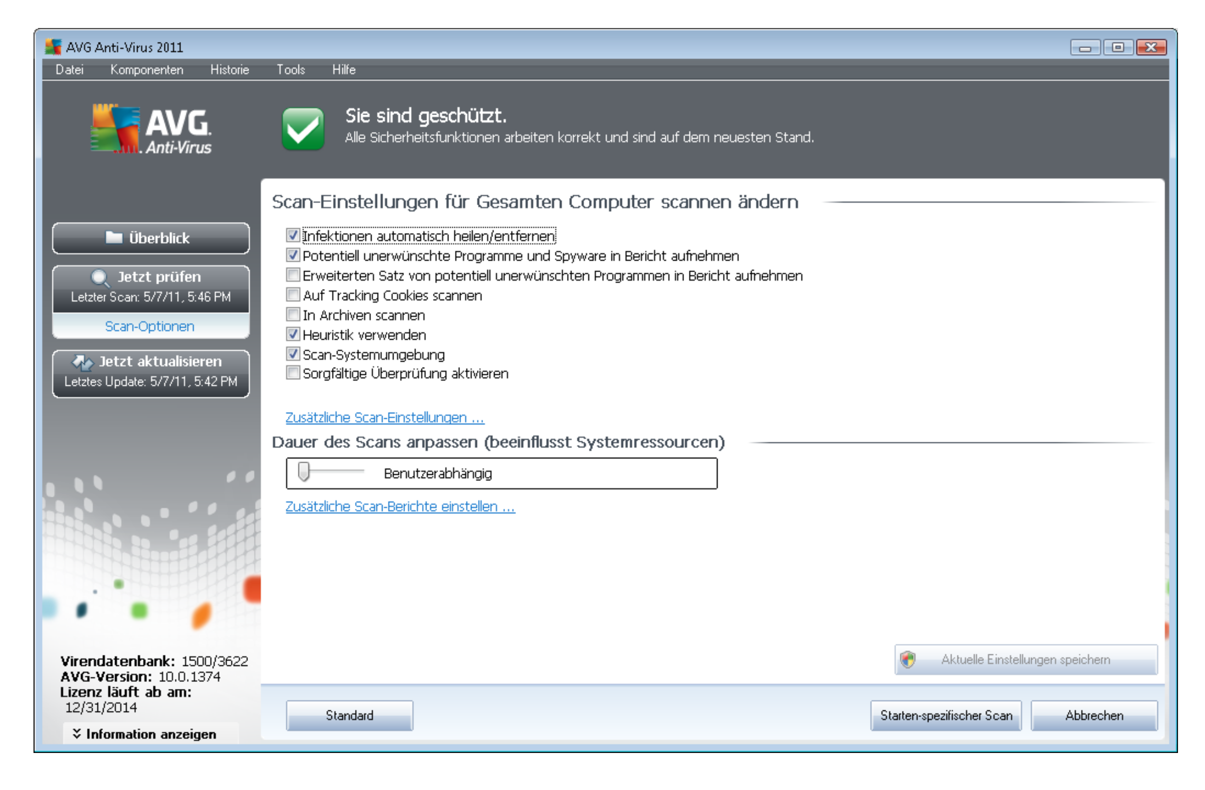




Bearbeitung der Scan-Konfiguration

Sie können die vordefinierten Standardeinstellungen der Option ***Scan des gesamten Computers*** bearbeiten. Klicken Sie auf den Link ***Scan-Einstellungen ändern***, um den Dialog ***Scan-Einstellungen für Scan des gesamten Computers ändern*** *zu öffnen (Zugriff über* *Benutzeroberfläche für Scans* *über den Link „Scan-Einstellungen ändern“ für* *Scan des gesamten Computers*). ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, Sie haben einen wichtigen Grund, sie zu ändern!***





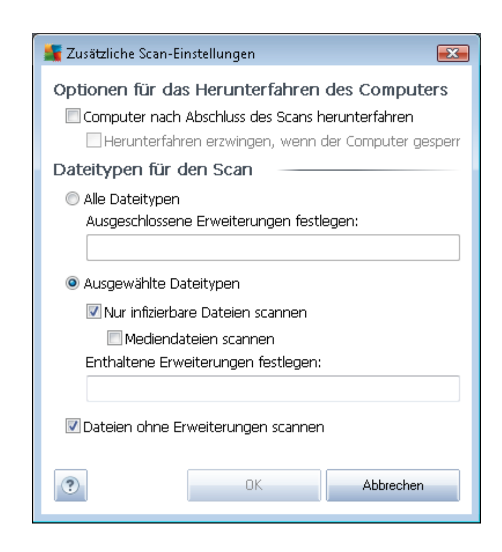
- ***Scan-Parameter*** – In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter ein- bzw. ausschalten:
    - ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die ***Virenquarantäne*** verschoben.
    - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
    - ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.
    - ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente ***Anti-Spyware*** legt fest, dass beim Scan Cookies erkannt werden



sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

- ***In Archiven scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.
- ***Heuristik verwenden*** (*standardmäßig aktiviert*) –·Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet.
- ***Scan-Systemumgebung*** (*standardmäßig aktiviert*) – Beim Scan werden auch die Systembereiche Ihres Computers überprüft.
- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog ***Zusätzliche Scan-Einstellungen*** geöffnet, in dem Sie die folgenden Parameter festlegen können:



- ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).
- ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:



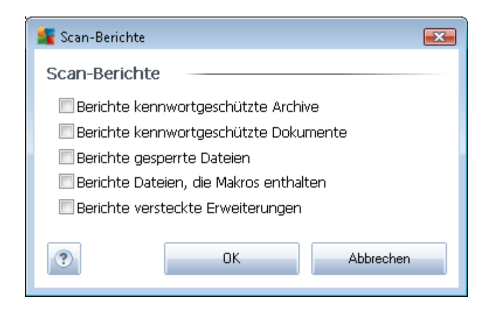
- ➢ ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;

- ➢ ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

- ➢ Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Dauer des Scans anpassen*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog **Scan-Berichte**, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:



Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel* ***AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen*** *beschrieben. Wenn Sie die Standardkonfiguration der Option* ***Gesamten Computer scannen*** *ändern, können Sie Ihre neuen Einstellungen als Standardkonfiguration speichern, die für alle weiteren Scans des gesamten Computers verwendet wird.*

10.2.2. Bestimmte Dateien/Ordner scannen

Bestimmte Dateien oder Ordner scannen – Scannt ausschließlich die Bereiche Ihres Computers, die Sie zum Scannen ausgewählt haben (*ausgewählte Ordner, Festplatten, Wechseldatenträger, CDs usw.*). Der Scan-Verlauf bei einer Virenerkennung sowie die Behandlung des Virus entsprechen



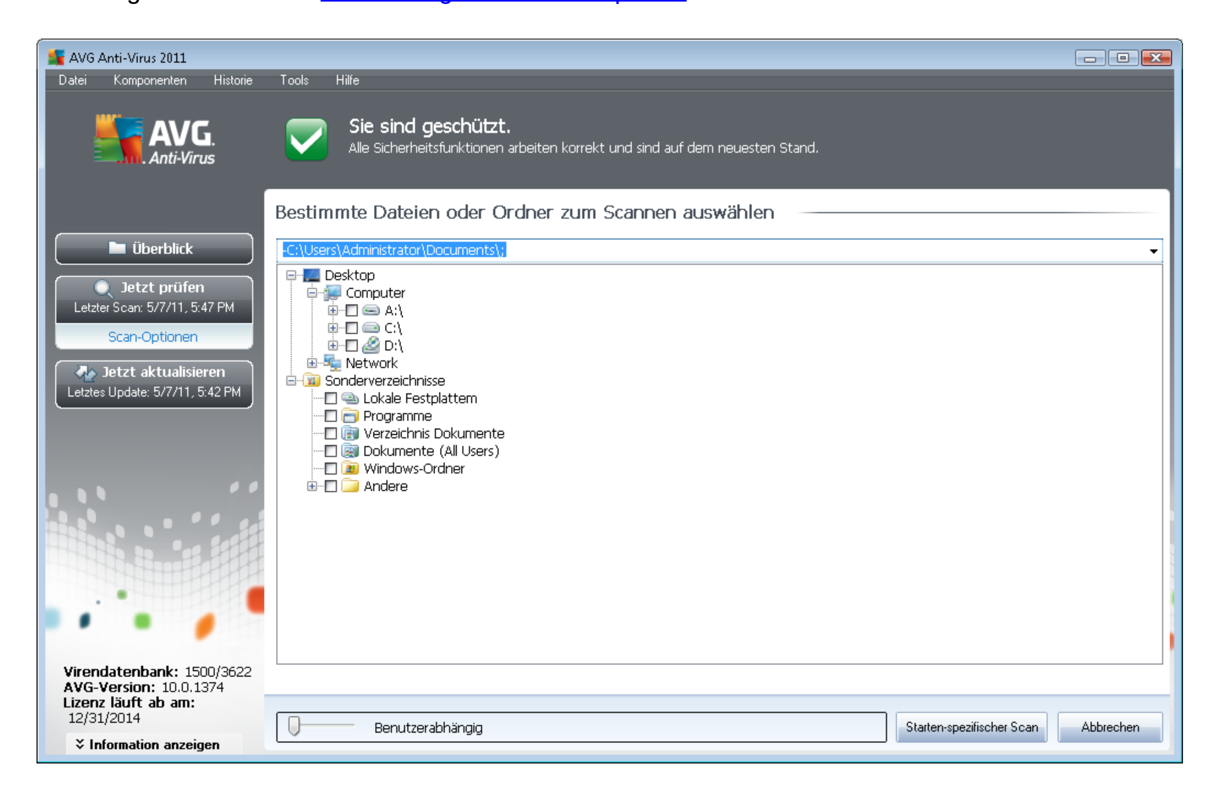
dem Scan des gesamten Computers***: Jedes gefundene Virus wird geheilt oder in die Virenquarantäne verschoben***. Das Scannen bestimmter Dateien oder Ordner kann verwendet werden, um eigene Scans und deren Zeitpläne nach Ihren Bedürfnissen einzurichten.

Start von Scans

Die Option ***Bestimmte Dateien/Ordner scannen*** kann direkt von der Benutzeroberfläche für Scans durch Klicken auf das Symbol des Scans gestartet werden. Es öffnet sich der Dialog ***Bestimmte Dateien oder Ordner zum Scannen auswählen***. Wählen Sie in der Baumstruktur Ihres Computers den zu scannenden Ordner aus. Der Pfad zu jedem Ordner wird automatisch generiert und wird in dem Textfeld im oberen Bereich dieses Dialogs angezeigt.

Es ist möglich, einen bestimmten Ordner zu scannen, jedoch seine Unterordner vom Scan auszuschließen. Setzen Sie dafür ein Minuszeichen „**-**" vor den automatisch generierten Pfad (*siehe Screenshot*). Um den gesamten Ordner vom Scan auszuschließen, verwenden Sie das Ausrufezeichen "!" parameter.

Klicken Sie zum Starten des Scans auf die Schaltfläche ***Scan starten***. Der Scanvorgang gleicht im Grunde genommen dem Scan des gesamten Computers.

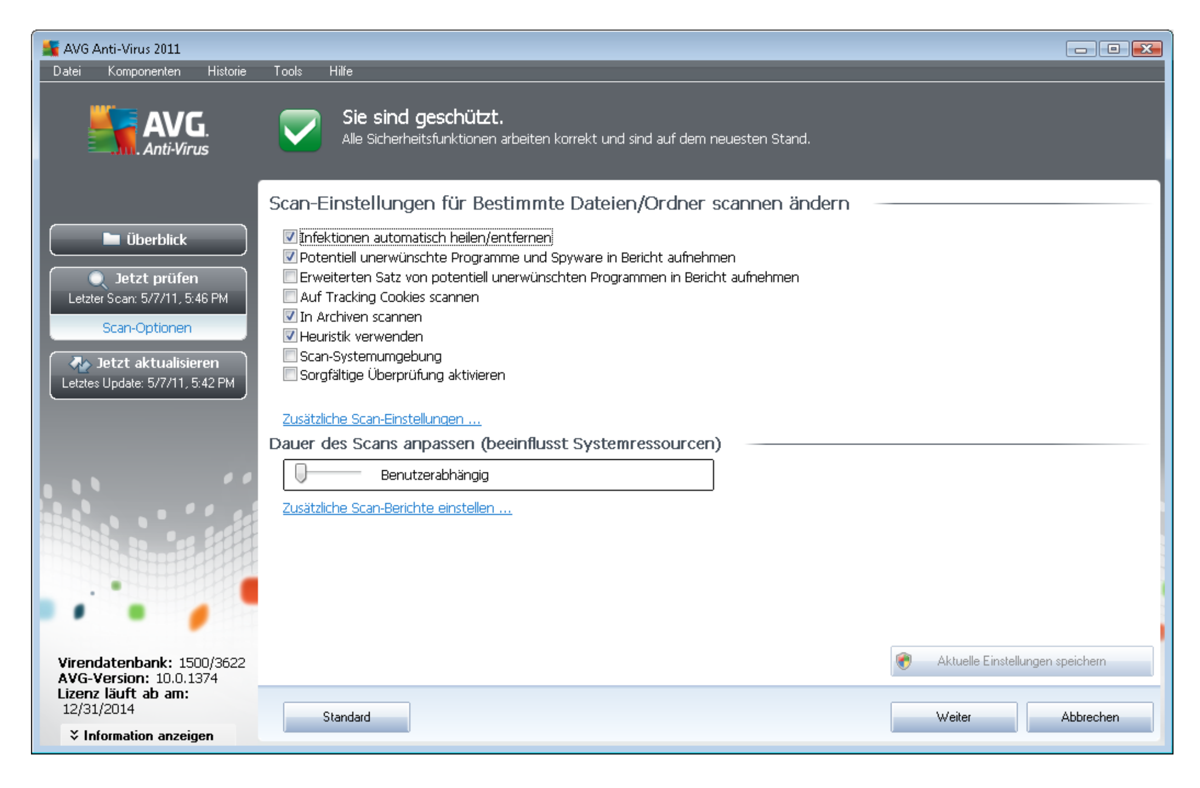


Bearbeitung der Scan-Konfiguration

Sie können die vordefinierten Standardeinstellungen der Option ***Bestimmte Dateien oder Ordner scannen*** bearbeiten. Klicken Sie auf den Link ***Scan-Einstellungen ändern*** , um den Dialog ***Scan-Einstellungen für Bestimmte Dateien/Ordner scannen ändern*** zu öffnen. ***Es empfiehlt sich, die Standardeinstellungen beizubehalten, es sei denn, Sie haben einen wichtigen Grund, sie zu***



ändern!



- ***Scan-Parameter*** – In der Liste der Scan-Parameter können Sie nach Bedarf bestimmte Parameter ein- bzw. ausschalten:
  - ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*) – Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann, wird das infizierte Objekt in die ***Virenquarantäne*** verschoben.
  - ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*) – Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.
  - ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.



- o ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*) – Dieser Parameter der Komponente [***Anti-Spyware***]() legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

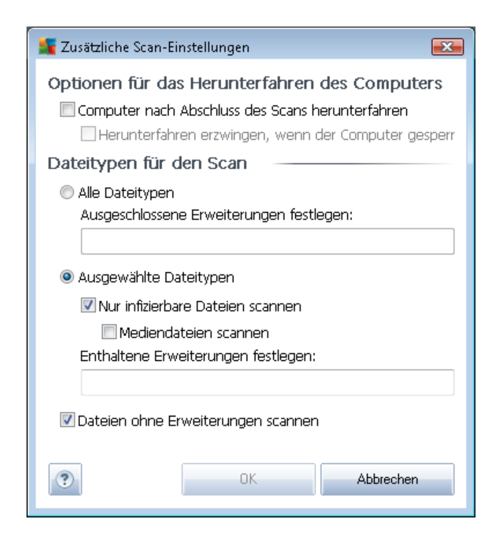
- o ***In Archiven scannen*** (*standardmäßig aktiviert*) – Dieser Parameter legt fest, dass beim Scan alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

- o ***Heuristik verwenden*** (*standardmäßig deaktiviert*) – Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet.

- o ***Scan-Systemumgebung*** (*standardmäßig deaktiviert*) –·Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

- o ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog ***Zusätzliche Scan-Einstellungen*** geöffnet, in dem Sie die folgenden Parameter festlegen können:



- o ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).

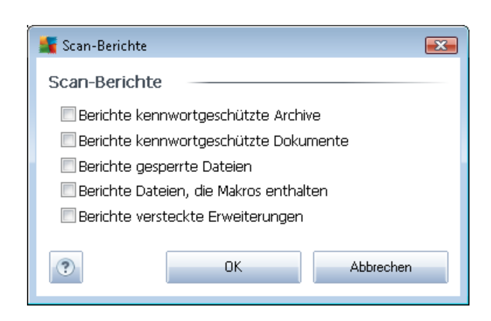
- o ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche



Elemente überprüft werden:

- ➢ ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;
- ➢ ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.
- ➢ Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Priorität des Scan-Vorgangs*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).
- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog ***Scan-Berichte***, wo Sie wählen können, welche Scan-Ergebnisse berichtet werden sollen:



Warnung: *Diese Scan-Einstellungen stimmen mit den Parametern eines neu definierten Scans überein. Diese werden im Kapitel* ***AVG Scan-Vorgang / Scan-Zeitpläne / Vorgehensweise beim Scannen*** *beschrieben. Wenn Sie die Standardkonfiguration der Option* ***Bestimmte Dateien oder Ordner scannen*** *ändern, können Sie Ihre neuen Einstellungen als Standardkonfiguration speichern, die für alle weiteren Scans bestimmter Dateien oder Ordner verwendet wird. Diese Konfiguration wird auch als Vorlage für alle Ihre neuen geplanten Scans verwendet (alle benutzerdefinierten Scans basieren auf der aktuellen Konfiguration des Scans bestimmter Dateien oder Ordner).*

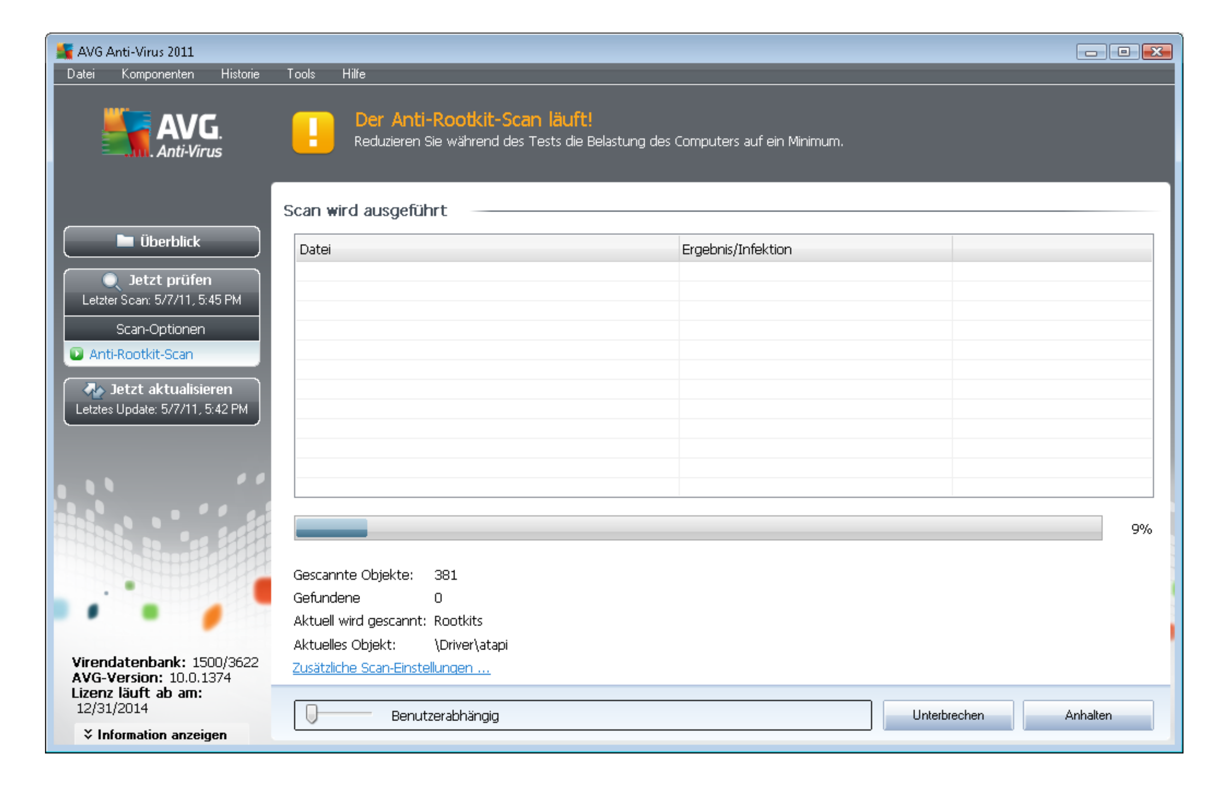


10.2.3. Anti-Rootkit-Scan

Anti-Rootkit-Scan überprüft Ihren Computer auf mögliche Rootkits (*Programme und Technologien, die Aktivitäten von Malware auf Ihrem Computer verbergen können*). Wenn ein Rootkit erkannt wird, heißt das nicht unbedingt, dass Ihr Computer infiziert ist. In manchen Fällen können bestimmte Treiber oder Abschnitte zulässiger Anwendungen fälschlicherweise als Rootkits erkannt werden.

Start von Scans

Anti-Rootkit-Scan können Sie direkt über die Benutzeroberfläche für Scans starten, indem Sie auf das Scan-Symbol klicken. Für diesen Scan-Typ müssen keine weiteren Einstellungen vorgenommen werden. Der Scan startet sofort im Dialog ***Scan wird ausgeführt*** (*siehe Screenshot*). Der Scanvorgang kann bei Bedarf unterbrochen (***Unterbrechen***) oder abgebrochen (***Anhalten***) werden.



Bearbeitung der Scan-Konfiguration

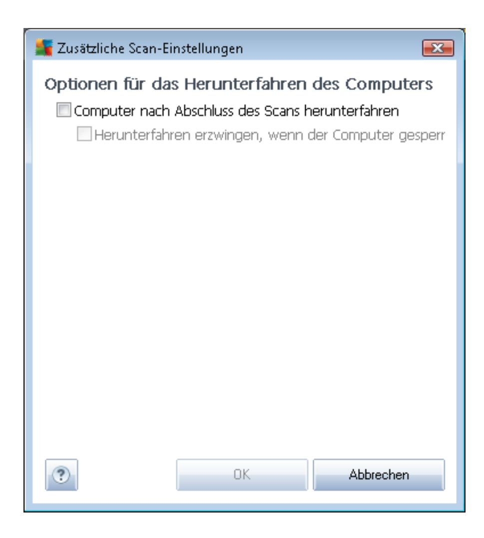
Anti-Rootkit-Scan wird stets mit den Standardeinstellungen gestartet; die Scanparameter können nur im Dialog ***Erweiterte Einstellungen von AVG/Anti-Rootkit*** bearbeitet werden. Auf der Scan-Oberfläche steht während der Ausführung eines Scans die folgende Konfiguration zur Verfügung:

- ***Automatischer Scan*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*).



Der Scan kann auch schneller ablaufen, wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

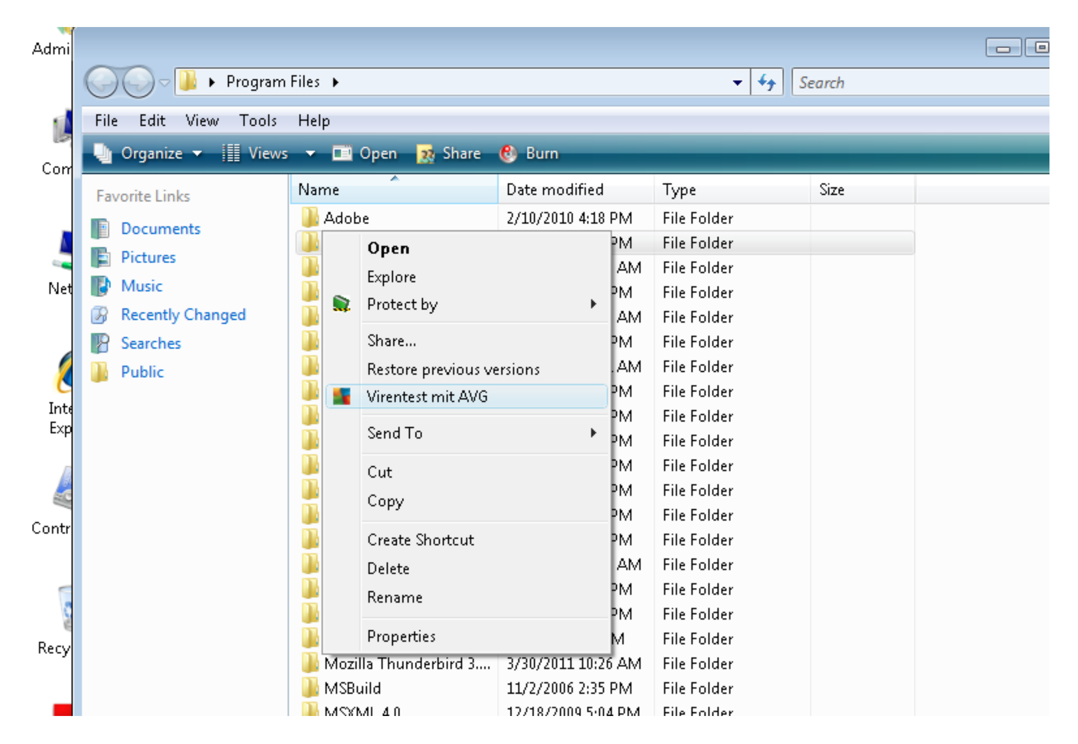
- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link lässt sich der Dialog ***Zusätzliche Scan-Einstellungen*** öffnen, in dem Sie mögliche Bedingungen für ein Herunterfahren des Computers im Hinblick auf den ***Anti-Rootkit-Scan*** festlegen können (***Computer nach Abschluss des Scans herunterfahren***, *möglicherweise* ***Herunterfahren erzwingen, wenn der Computer gesperrt ist***):



10.3. Scans aus dem Windows Explorer

Neben den vordefinierten Scans, die für den gesamten Computer oder ausgewählte Bereiche gestartet werden, umfasst **AVG Anti-Virus 2011** auch eine Option für die Schnellprüfung eines bestimmten Objekts direkt in Windows Explorer. Wenn Sie eine unbekannte Datei öffnen und ihren Inhalt nicht genau kennen, möchten Sie sie möglicherweise On-Demand überprüfen. Gehen Sie dazu wie folgt vor:





- Markieren Sie im Windows Explorer die Datei (oder den Ordner), die Sie überprüfen möchten

- Klicken Sie mit der rechten Maustaste auf das Objekt, um das Kontextmenü zu öffnen

- Wählen Sie die Option ***Virentest mit AVG Anti-Virus***, um die Datei mit AVG zu scannen

10.4. Scannen von Befehlszeilen

Mit **AVG Anti-Virus 2011** haben Sie die Möglichkeit, einen Scan von der Befehlszeile aus durchzuführen. Diese Option kann beispielsweise für Server oder für die Erstellung eines Batch-Skripts angewendet werden, das nach dem Hochfahren des Computers automatisch gestartet werden soll. Wenn Sie einen Scan von der Befehlszeile aus durchführen, können Sie einen Großteil der Parameter anwenden, die auch in der Benutzeroberfläche von AVG zur Verfügung stehen.

Um einen AVG-Scan von der Befehlszeile aus zu starten, führen Sie den folgenden Befehl in dem Ordner aus, in dem AVG installiert wurde:

- ***avgscanx*** für 32-Bit-Betriebssysteme

- ***avgscana*** für 64-Bit-Betriebssysteme

Syntax des Befehls

Die Syntax des Befehls lautet:

- ***avgscanx /Parameter*** ... z. B. ***avgscanx /comp***, um den gesamten Computer zu scannen



- ***avgscanx /Parameter /Parameter*** .. Wenn mehrere Parameter verwendet werden, müssen diese in einer Reihe geschrieben und mit einem Leerzeichen und einem Schrägstrich getrennt werden.

- Wenn ein Parameter einen bestimmten Wert erfordert (der Parameter ***/scan*** benötigt z. B. Informationen über die Bereiche Ihres Computers, die gescannt werden sollen, und die genaue Pfadangabe zum ausgewählten Bereich), werden die einzelnen Werte durch Semikola getrennt, z. B.: ***avgscanx /scan=C:\;D:***

Scan-Parameter

Um eine vollständige Übersicht der verfügbaren Parameter anzuzeigen, geben Sie den entsprechenden Befehl mit dem Parameter /? oder /HELP ein (z. B. ***avgscanx /?***). Der einzige obligatorische Parameter ist /SCAN, mit dem festgelegt wird, welche Bereiche des Computers gescannt werden sollen. Eine genauere Erläuterung der Optionen finden Sie in der Übersicht zu Befehlszeilenparametern.

Drücken Sie die ***Eingabetaste***, um den Scan auszuführen. Der Scanvorgang kann mit den Tastenkombinationen ***Strg+C*** oder ***Strg+Pause*** abgebrochen werden.

CMD-Scan über die Benutzeroberfläche starten

Wenn Ihr Computer im abgesicherten Modus arbeitet, können Sie den Befehlszeilen-Scan auch über die grafische Benutzeroberfläche starten. Der Scan selbst wird von der Befehlszeile aus gestartet. Im Dialog ***Erstellungshilfe über die Befehlszeile*** können Sie nur die meisten Scan-Parameter in der übersichtlichen Benutzeroberfläche festlegen.

Da der Zugriff auf diesen Dialog nur im abgesicherten Modus von Windows möglich ist, können Sie sich genauere Informationen zu diesem Dialog in der Hilfedatei ansehen, die direkt in diesem Dialog geöffnet werden kann.

10.4.1. Parameter für CMD-Scan

Die folgende Liste enthält alle Parameter, die zum Scannen von der Befehlszeile aus zur Verfügung stehen:

- ***/SCAN*** Bestimmte Dateien/ Ordner scannen /SCAN=path;path (e.g. /SCAN=C:\;D:\)
- ***/COMP*** Scan des gesamten Computers
- ***/HEUR*** Heuristische Analyseverwenden
- ***/EXCLUDE*** Pfad oder Datei(en) vom Scan ausschließen
- ***/@*** Befehlsdatei /Dateiname/
- ***/EXT*** Diese Erweiterungen scannen /z. B. EXT=EXE,DLL/



- ***/NOEXT*** Diese Erweiterungen nicht scannen /z. B. NOEXT=JPG/
- ***/ARC*** Archive scannen
- ***/CLEAN*** Automatisch bereinigen
- ***/TRASH*** Infizierte Dateien in die Virenquarantäne verschieben
- ***/QT*** Schnelltest
- ***/MACROW*** Makros in Bericht aufnehmen
- ***/PWDW*** Kennwortgeschützte Dateien in Bericht aufnehmen
- ***/IGNLOCKED*** Gesperrte Dateien ignorieren
- ***/REPORT*** Bericht in Datei /Dateiname/
- ***/REPAPPEND*** An die Berichtsdatei anhängen
- ***/REPOK*** Nicht infizierte Dateien als OK in Bericht aufnehmen
- ***/NOBREAK*** Kein Abbrechen mit STRG-PAUSE
- ***/BOOT*** MBR/BOOT-Test aktivieren
- ***/PROC*** Aktive Prozesse scannen
- ***/PUP*** „Potentiell unerwünschte Programme" in Bericht aufnehmen
- ***/REG*** Registry scannen
- ***/COO*** Cookies scannen
- ***/?*** Hilfe zu diesem Thema anzeigen
- ***/HELP*** Hilfe zu diesem Thema anzeigen
- ***/PRIORITY*** Scan-Priorität einstellen /Niedrig, Auto, Hoch/ (siehe Erweiterte Einstellungen/Scans)
- ***/SHUTDOWN*** Computer nach Abschluss des Scans herunterfahren
- ***/FORCESHUTDOWN*** Herunterfahren erzwingen, wenn der Scan abgeschlossen ist
- ***/ADS*** Alternative Datenströme scannen (nur NTFS)
- ***/ARCBOMBSW*** Erneut komprimierte Archivdateien melden

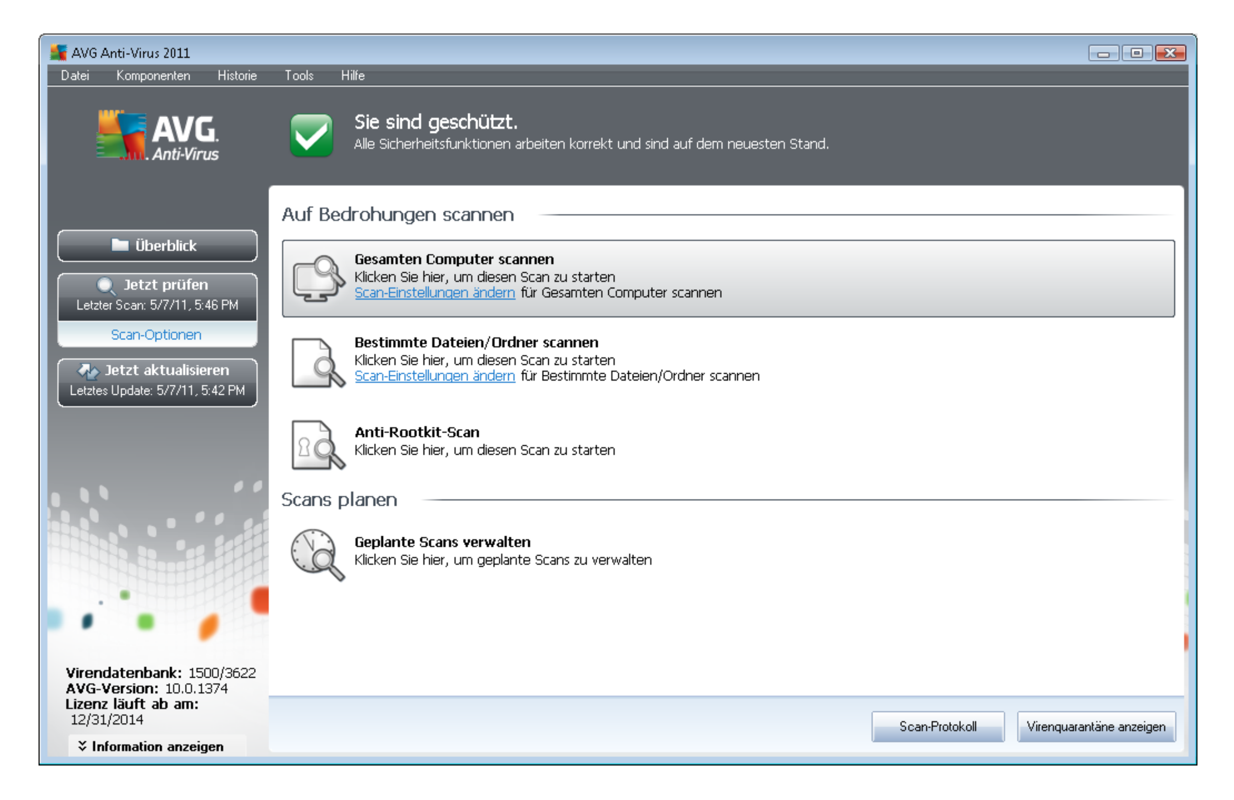


10.5. Scans planen

Mit **AVG Anti-Virus 2011** können Sie On-Demand-Scans (z. B. wenn Sie befürchten, dass Ihr Computer infiziert wurde) oder einen geplanten Scan ausführen. Es wird dringend empfohlen, geplante Scans auszuführen. Auf diese Weise sorgen Sie dafür, dass Ihr Computer gegen Infektionen geschützt ist, und Sie müssen sich nicht darum kümmern, ob und wann ein Scan gestartet werden soll.

Sie sollten die Funktion ***Scan des gesamten Computers*** regelmäßig, mindestens einmal pro Woche, starten. Wenn möglich, sollten Sie Ihren gesamten Computer täglich scannen. Dies ist auch die Standardkonfiguration für geplante Scans. Wenn der Computer immer eingeschaltet ist, können Sie die Scans für Zeiten außerhalb der Arbeitszeit planen. Wenn der Computer manchmal ausgeschaltet ist, werden die geplanten Scans beim Start des Computers ausgeführt, wenn eine Aufgabe verpasst wurde.

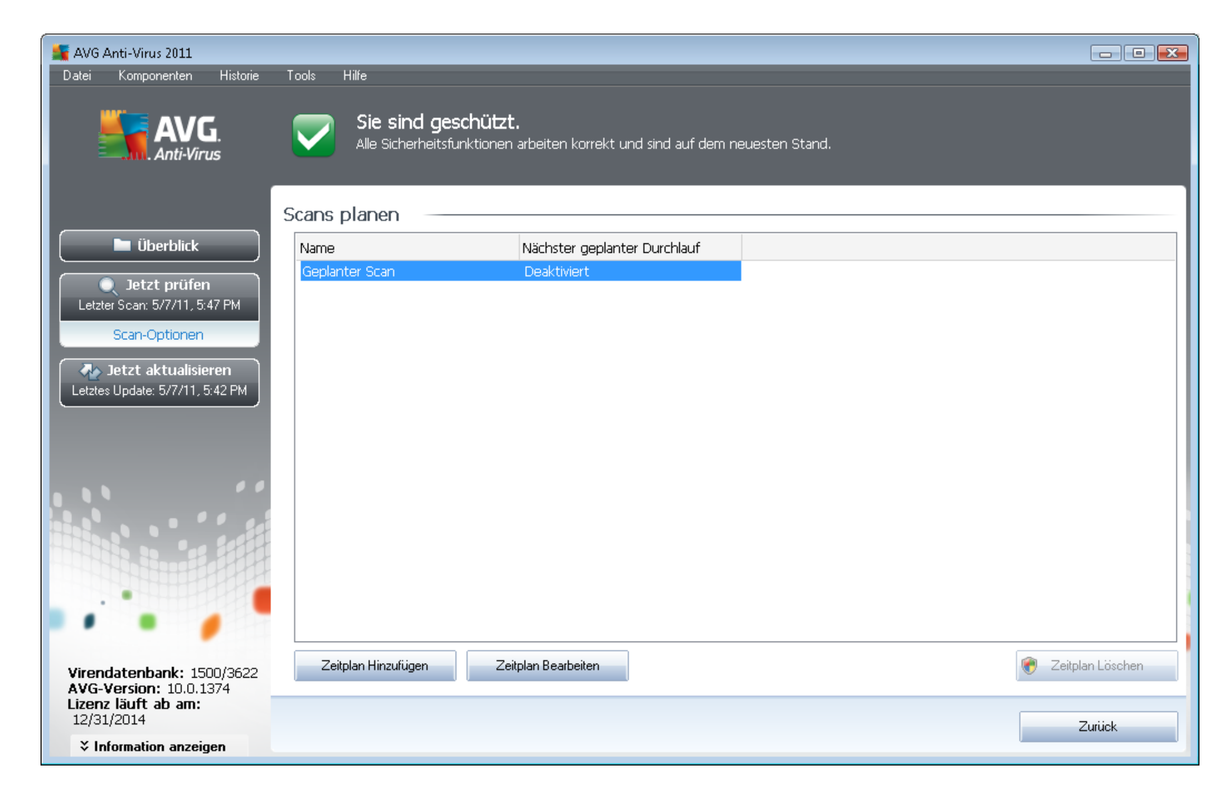
Um neue Span-Pläne zu erstellen, gehen Sie auf der Scan-Oberfläche von AVG unten zum Abschnitt ***Scans planen***:



Scans planen

Klicken Sie im Bereich ***Scans planen*** auf das grafische Symbol, um den Dialog ***Scans planen*** zu öffnen, in dem eine Liste aller gegenwärtig geplanten Scans angezeigt wird:





Sie können Scans mithilfe der folgenden Schaltflächen bearbeiten oder hinzufügen:

- ***Zeitplan Hinzufügen*** – Mit dieser Schaltfläche wird der Dialog ***Einstellungen für geplanten Scan*** auf dem Reiter ***Einstellungen für den Zeitplan*** geöffnet. In diesem Dialog können Sie die Parameter für den neu definierten Scan festlegen.

- ***Zeitplan Bearbeiten*** – Diese Schaltfläche steht nur zur Verfügung, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. In diesem Fall ist die Schaltfläche aktiv, und Sie können darauf klicken, um zum Dialog ***Einstellungen für geplanten Scan*** auf dem Reiter ***Einstellungen für den Zeitplan*** zu wechseln. Hier sind bereits Parameter des ausgewählten Scans festgelegt und können bearbeitet werden.

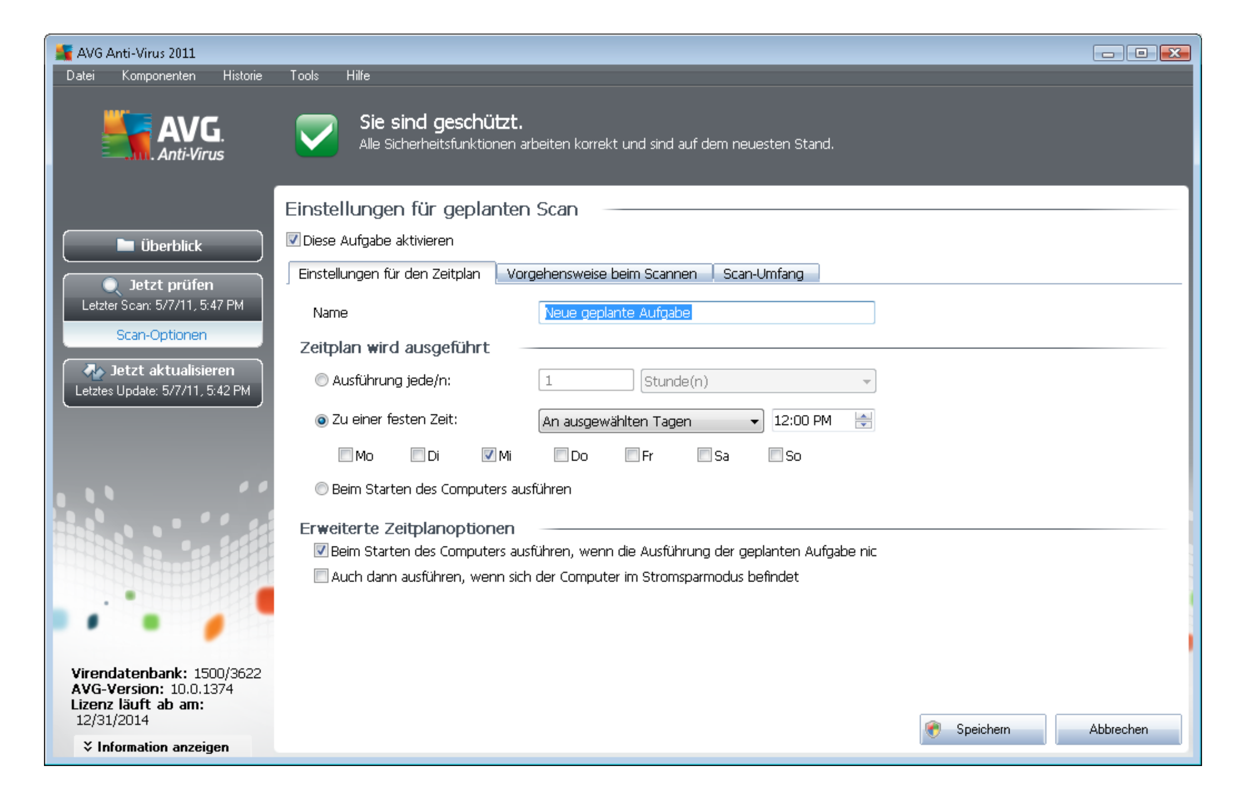
- ***Zeitplan Löschen*** – Diese Schaltfläche ist ebenfalls nur aktiv, wenn Sie bereits vorher einen bestehenden Scan aus der Liste der geplanten Scans ausgewählt haben. Dieser Scan wird durch Klicken auf die Schaltfläche aus der Liste gelöscht. Sie können jedoch nur Ihre eigenen Scans entfernen. Der ***Zeitplan für Scans des gesamten Computers***, der in den Standardeinstellungen vordefiniert ist, kann nicht gelöscht werden.

- ***Zurück*** – Zurück zur Scan-Oberfläche von AVG

10.5.1. Einstellungen für den Zeitplan

Wenn Sie einen neuen Test und dessen regulären Start planen möchten, machen Sie im Dialog ***Einstellungen für geplanten Test*** die entsprechenden Angaben (*Klicken Sie im Dialog **Scans planen** auf die Schaltfläche **Scan-Zeitplan hinzufügen***). Der Dialog ist in drei Reiter unterteilt: ***Einstellungen für den Zeitplan*** – *siehe Bild unten (Der Standardreiter, zu dem Sie automatisch weitergeleitet werden)*, ***Vorgehensweise beim Scannen*** und ***Scan-Umfang***.





Auf dem Reiter ***Einstellungen für den Zeitplan*** können Sie den Eintrag ***Diese Aufgabe aktivieren*** aktivieren oder deaktivieren, um den geplanten Scan vorübergehend zu deaktivieren. Anschließend können Sie den Zeitplan bei Bedarf wieder aktivieren.

Geben Sie anschließend dem zu erstellenden und zu planenden Scan einen Namen. Geben Sie den Namen im Textfeld ***Name*** ein. Wählen Sie nach Möglichkeit kurze, beschreibende Namen für Ihre Scans, damit Sie die einzelnen Scans später leichter unterscheiden und wiederfinden können.

Beispiel: *Sie sollten einen Scan nicht „Neuer Scan“ oder „Mein Scan“ nennen, da diese Namen nichts darüber aussagen, was der Scan tatsächlich überprüft. Ein Beispiel für einen guten, beschreibenden Namen wäre andererseits „Scan von Systembereichen“ usw. Es ist auch nicht erforderlich, im Namen des Scans anzugeben, ob es sich um einen Scan des gesamten Computers handelt oder lediglich um den Scan bestimmter Dateien oder Ordner. Ihre eigenen Scans sind immer bestimmte Versionen eines [Scans bestimmter Dateien oder Ordner](#).*

In diesem Dialog können Sie weiterhin folgende Parameter für den Scan festlegen:

- ***Zeitplan wird ausgeführt*** – Legen Sie das Zeitintervall für den Start des neu geplanten Scans fest. Sie können entweder wiederholte Starts des Scans nach einem bestimmten Zeitraum·(***Ausführung jede/n***) oder ein exaktes Datum und eine Uhrzeit (***Zu einer festen Zeit***) oder ein Ereignis festlegen, das den Start eines Scans auslösen soll (In Abhängigkeit von einer bestimmten Aktion: ***Beim Start des Computers***).

- ***Erweiterte Zeitplanoptionen*** – In diesem Bereich können Sie festlegen, unter welchen Bedingungen der Scan gestartet/nicht gestartet werden soll, wenn sich der Computer im Stromsparmodus befindet oder vollständig ausgeschaltet ist.



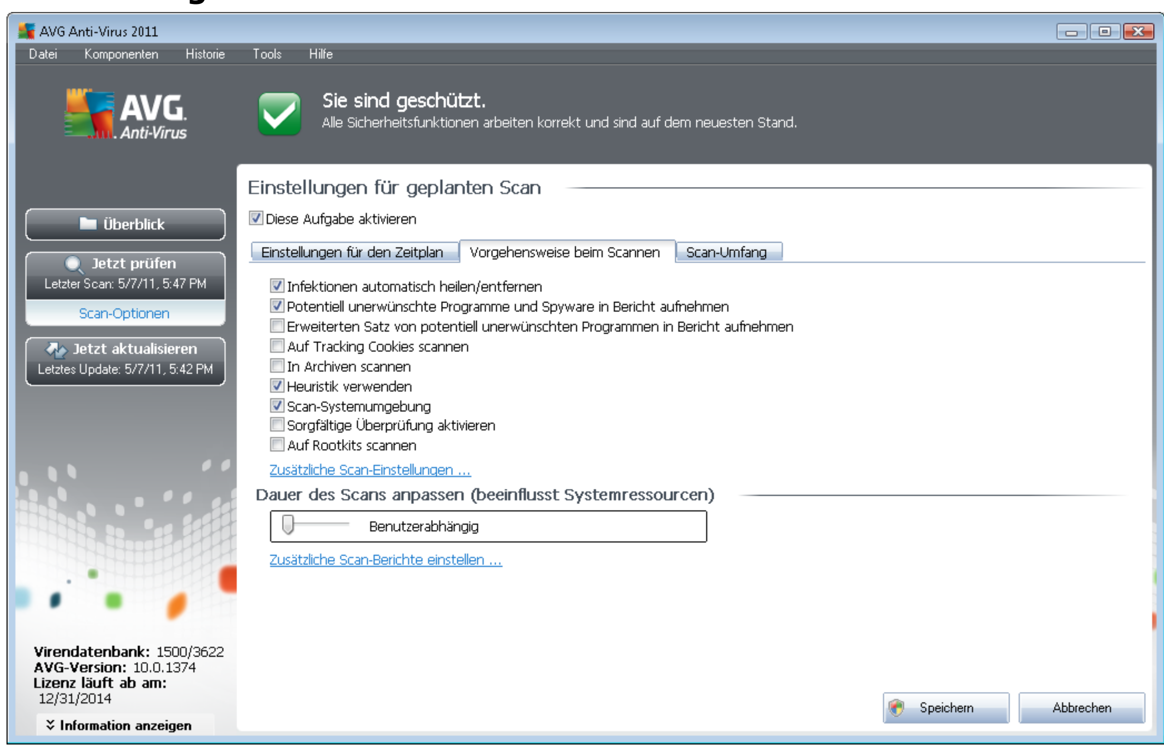
Schaltflächen im Dialog „Einstellungen für geplanten Scan“

Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Scan-Umfang***) zwei Schaltflächen zur Verfügung, die auf allen Reitern dieselbe Funktion haben:

- ***Übernehmen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.

10.5.2. Vorgehensweise beim Scannen



Der Reiter ***Vorgehensweise beim Scannen*** enthält eine Liste der Scan-Parameter, die optional aktiviert oder deaktiviert werden können. Standardmäßig sind die meisten Parameter aktiviert und ihre Funktionen werden während des Scans angewandt. Wenn Sie keinen wichtigen Grund haben, diese Einstellungen zu ändern, empfehlen wir Ihnen, die vordefinierte Konfiguration beizubehalten:

- ***Infektionen automatisch heilen/entfernen*** (*standardmäßig aktiviert*): Wenn beim Scan ein Virus erkannt wird, wird die Infektion automatisch geheilt, sofern eine Gegenmaßnahme zur Verfügung steht. Wenn die infizierte Datei nicht automatisch geheilt werden kann oder wenn



Sie diese Option deaktivieren, werden Sie über einen Virenfund unterrichtet, und Sie können entscheiden, was mit der erkannten Infektion geschehen soll. Es wird empfohlen, die infizierte Datei in die ***Virenquarantäne*** zu verschieben.

- ***Potentiell unerwünschte Programme und Spyware in Bericht aufnehmen*** (*standardmäßig aktiviert*): Aktivieren Sie dieses Kontrollkästchen, um die ***Anti-Spyware***-Engine zu aktivieren und auf Spyware sowie Viren zu scannen. Spyware stellt eine fragwürdige Malware-Kategorie dar: Obwohl Spyware normalerweise ein Sicherheitsrisiko bedeutet, können einige dieser Programme absichtlich installiert werden. Wir empfehlen, diese Funktion nicht zu deaktivieren, um die Sicherheit Ihres Computers zu gewährleisten.

- ***Erweiterten Satz von potentiell unerwünschten Programmen in Bericht aufnehmen*** (*standardmäßig deaktiviert*): Aktivieren Sie diese Option, um ein erweitertes Paket von Spyware zu erkennen: Programme, die harmlos sind, wenn Sie sie direkt vom Hersteller erhalten, die jedoch zu einem späteren Zeitpunkt zu Schadenszwecken missbraucht werden können. Dies stellt eine zusätzliche Maßnahme für eine erhöhte Sicherheit Ihres Computers dar. Es können jedoch legale Programme blockiert werden, weshalb diese Option standardmäßig ausgeschaltet ist.

- ***Auf Tracking Cookies scannen*** (*standardmäßig deaktiviert*): Dieser Parameter der Komponente ***Anti-Spyware*** legt fest, dass beim Scan Cookies erkannt werden sollen (*HTTP-Cookies werden zur Authentifizierung, zum Verfolgen und Erhalt bestimmter Benutzerinformationen verwendet, wie beispielsweise Vorlieben und Inhalte von Warenkörben*).

- ***In Archiven scannen*** (*standardmäßig deaktiviert*): Dieser Parameter legt fest, dass bei Scans alle Dateien überprüft werden sollen, selbst solche, die in Archiven (wie ZIP, RAR usw.) gespeichert sind.

- ***Heuristik verwenden*** (*standardmäßig aktiviert*): Beim Scan wird zur Virenerkennung unter anderem die heuristische Analyse (*eine dynamische Emulation der Anweisungen des gescannten Objekts in einer virtuellen Computerumgebung*) verwendet.

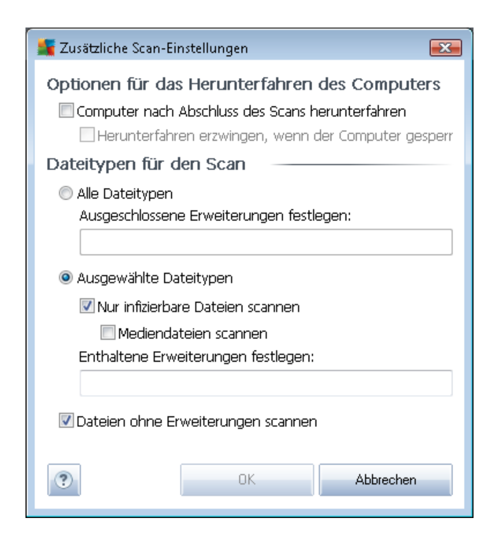
- ***Scan-Systemumgebung*** (*standardmäßig aktiviert*): Beim Scan werden auch die Systembereiche Ihres Computers überprüft.

- ***Sorgfältige Überprüfung aktivieren*** (*standardmäßig deaktiviert*) – Aktivieren Sie diese Option in bestimmten Situationen (*z. B. wenn Sie glauben, dass Ihr Computer infiziert wurde*), um einen sorgfältigen Scan zu starten, bei dem zur Sicherheit auch Bereiche Ihres Computers gescannt werden, die selten infiziert werden. Beachten Sie, dass dieser Scan recht zeitaufwendig ist.

Anschließend können Sie die Scan-Konfiguration wie folgt ändern:

- ***Zusätzliche Scan-Einstellungen*** – Mit diesem Link wird der Dialog ***Zusätzliche Scan-Einstellungen*** geöffnet, in dem Sie die folgenden Parameter festlegen können:





- o ***Optionen für das Herunterfahren des Computers*** – Hier können Sie festlegen, ob der Computer nach dem Abschluss des Scanvorgangs automatisch heruntergefahren werden soll. Mit der Bestätigung dieser Option (***Computer nach Abschluss des Scans herunterfahren***) wird eine neue Option aktiviert, durch die der Computer heruntergefahren wird, auch wenn er gesperrt ist (***Herunterfahren erzwingen, wenn der Computer gesperrt ist***).

- o ***Dateitypen für den Scan festlegen*** – Außerdem sollten Sie bestimmen, welche Elemente überprüft werden:

  - ➢ ***Alle Dateitypen*** mit der Möglichkeit, Ausnahmen für den Scanvorgang festzulegen, indem Sie eine Liste mit durch Kommata getrennten Dateierweiterungen erstellen, die nicht überprüft werden sollen;

  - ➢ ***Ausgewählte Dateitypen*** – Wenn Sie diese Option aktivieren, werden nur potentiell infizierbare Dateien gescannt (*Dateien, die nicht infiziert werden können, wie einfache Textdateien oder andere nicht ausführbare Dateien, werden nicht gescannt*), darunter Mediendateien (*Video- und Audiodateien – wenn das Kontrollkästchen deaktiviert bleibt, ist die Scanzeit erheblich kürzer, da diese Dateien oft sehr groß und nur selten mit Viren infiziert sind*). Auch hier können Sie anhand der Erweiterungen festlegen, welche Dateien in jedem Fall überprüft werden sollen.

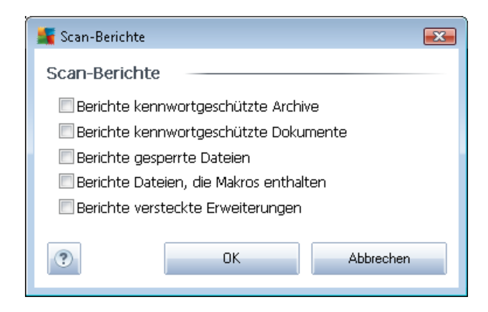
  - ➢ Auf Wunsch können Sie auch ***Dateien ohne Erweiterungen scannen*** – Diese Option ist standardmäßig aktiviert, und wir empfehlen Ihnen, diese Konfiguration nur dann zu ändern, wenn Sie einen guten Grund dafür haben. Dateien ohne Erweiterungen sind generell verdächtig und sollten auf jeden Fall gescannt werden.

- ***Dauer des Scans anpassen*** – Mit dem Schieberegler können Sie die Priorität des Scanvorgangs ändern. Standardmäßig ist dieser Optionswert auf die Stufe *Benutzerabhängig* der automatischen Ressourcennutzung eingestellt. Alternativ können Sie den Scanvorgang auch langsamer ablaufen lassen, wodurch die Systemressourcenbelastung minimiert wird (*nützlich, wenn Sie am Computer arbeiten und Ihnen die Dauer des Scans nicht wichtig ist*). Der Scan kann auch schneller ablaufen,



wodurch die Systemressourcenbelastung erhöht wird (*z. B. wenn am Computer zeitweise nicht gearbeitet wird*).

- ***Zusätzliche Scan-Berichte einstellen*** – Dieser Link öffnet den Dialog ***Scan-Berichte***, in dem Sie wählen können, über welche Scan-Ergebnisse Sie informiert werden möchten:



Hinweis:*Standardmäßig ist die Scan-Konfiguration so eingestellt, dass eine optimale Leistung erzielt wird. Wenn Sie keinen wichtigen Grund haben, die Scan-Einstellungen zu ändern, wird dringend empfohlen, die vordefinierte Konfiguration beizubehalten. Änderungen an der Konfiguration sollten nur von erfahrenen Benutzern durchgeführt werden. Weitere Optionen für die Scan-Konfiguration finden Sie im Dialog* ***Erweiterte Einstellungen****, den Sie über das Systemmenü mit* ***Tools/ Erweiterte Einstellungen*** *aufrufen können.*

Schaltflächen

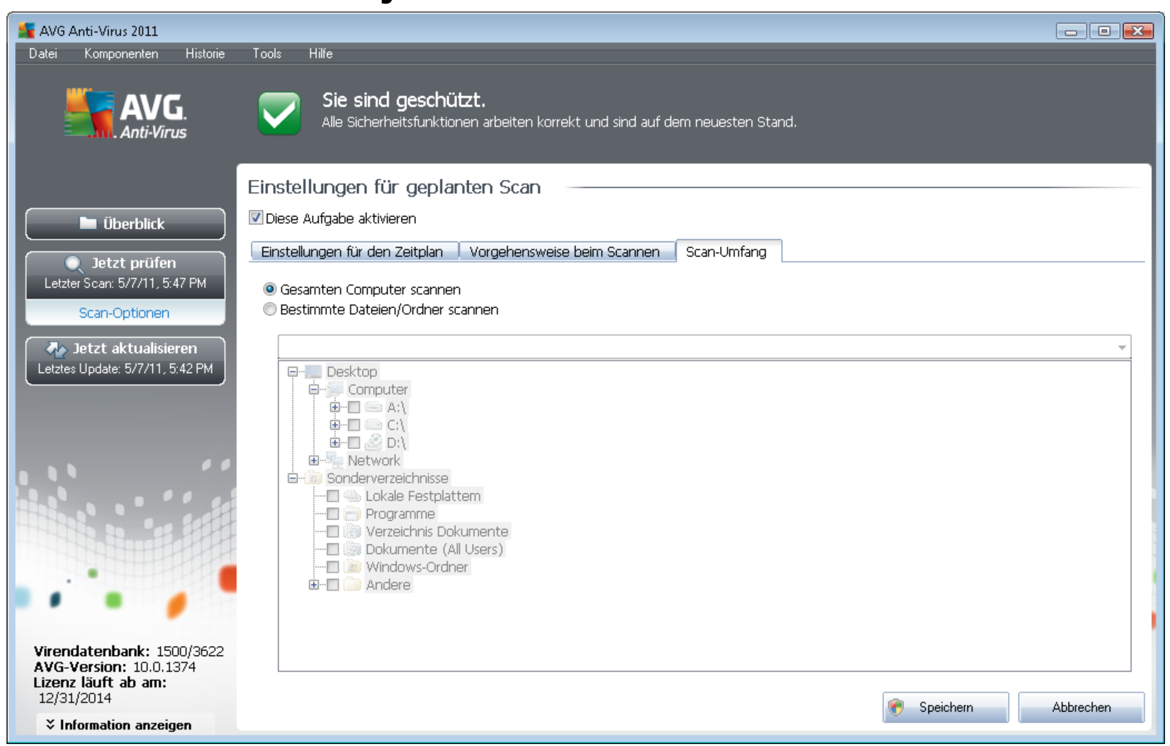
Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Scan-Umfang***) zwei Schaltflächen zur Verfügung, die auf allen Reitern dieselbe Funktion haben:

- ***Übernehmen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.



10.5.3. Zu testende Objekte



Auf dem Reiter ***Scan-Umfang*** können Sie festlegen, ob Sie die Option Gesamten Computer scannen oder Bestimmte Dateien oder Ordner scannen planen möchten.

Wenn Sie die Option „Bestimmte Dateien oder Ordner scannen" auswählen, wird im unteren Bereich dieses Dialogs die angezeigte Baumstruktur aktiviert, und Sie können die zu scannenden Ordner festlegen. (*Sie können Elemente einblenden, indem Sie auf das Plus-Zeichen klicken, bis Sie den zu scannenden Ordner finden.*) Sie können mehrere Ordner auswählen, indem Sie die entsprechenden Kästchen aktivieren. Die ausgewählten Ordner erscheinen im Textfeld im oberen Bereich des Dialogs. Im Dropdown-Menü wird Ihr Scanverlauf für einen späteren Gebrauch festgehalten. Alternativ können Sie den vollständigen Pfad zu dem gewünschten Ordner manuell eingeben (*bei mehreren Pfaden müssen diese mit einem Semikolon ohne Leerzeichen voneinander getrennt werden*).

Innerhalb der Baumstruktur sehen Sie einen Zweig namens ***Spezielle Speicherorte***. Im Folgenden wird eine Liste mit Speicherorten aufgeführt, die nach Aktivierung des entsprechenden Kontrollkästchens gescannt werden:

- ***Lokale Festplatten*** – alle Festplatten Ihres Computers
- ***Programmdateien***
  - o C:\Programme\
  - o *in 64-Bit-Versionen* C:\Programme (x86)
- ***Ordner „Eigene Dateien"***



   - *unter Windows XP*: C:\Dokumente und Einstellungen\Standardbenutzer\Eigene Dateien\
   - *unter Windows Vista/7*: C:\Benutzer\"Benutzername"\Dokumente\

- ***Gemeinsame Dokumente***
   - *unter Windows XP:* : C:\Dokumente und Einstellungen\Alle Benutzer\Dokumente\
   - *unter Windows Vista/7*: C:\Benutzer\Öffentlich\Dokumente\

- ***Windows-Ordner*** – C:\Windows\

  - ***Andere***
     - *Systemlaufwerk* – die Festplatte, auf der das Betriebssystem installiert ist (normalerweise C:)
     - *Systemordner* – C:\Windows\System32\
     - *Ordner „Temporäre Dateien“* – C:\Dokumente und Einstellungen\Benutzer\Lokal (*Windows XP*oder C:\Benutzer\"Benutzername"\AppData\Local\Temp *Windows Vista/7*)
     - *Temporäre Internetdateien* – C:\Dokumente und Einstellungen\Benutzer\Lokale Einstellungen\Temporäre Internetdateien\ (*Windows XP*) oder C:\Benutzer\"Benutzername"\AppData\Local\Microsoft\Windows\Temporäre Internetdateien (*Windows Vista/7*)

Schaltflächen im Dialog „Einstellungen für geplanten Scan“

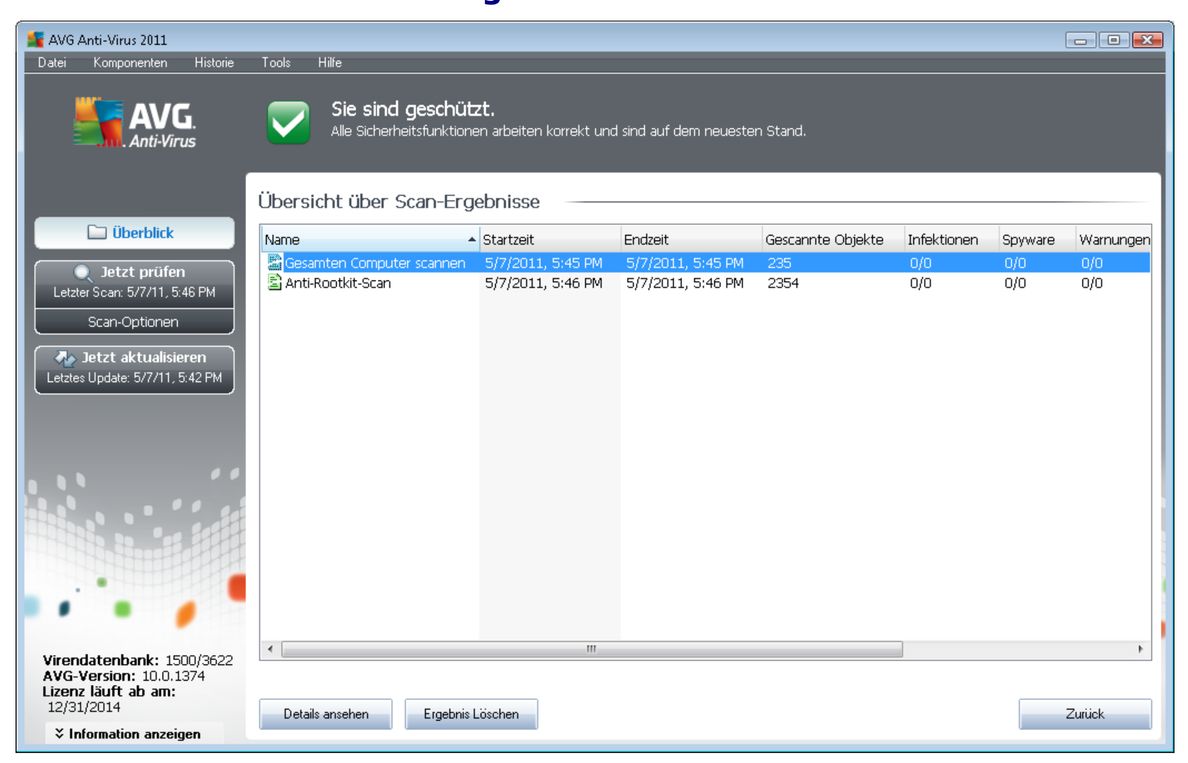
Im Dialog ***Einstellungen für geplanten Scan*** stehen auf allen drei Reitern (***Einstellungen für den Zeitplan***, ***Vorgehensweise beim Scannen*** und ***Scan-Umfang***) zwei Schaltflächen zur Verfügung, die auf allen Reitern dieselbe Funktion haben:

- ***Übernehmen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden gespeichert, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG. Wenn Sie daher die Parameter des Scans auf allen Reitern konfigurieren möchten, klicken Sie erst auf diese Schaltfläche, nachdem Sie alle Anforderungen festgelegt haben.

- ***Abbrechen*** – Alle Änderungen, die Sie auf diesem Reiter oder auf einem anderen Reiter dieses Dialogs vorgenommen haben, werden abgebrochen, und der Dialog wechselt zum Standarddialog der Scan-Oberfläche von AVG.



10.6. Übersicht über Scan-Ergebnisse



Der Dialog ***Übersicht über Scan-Ergebnisse*** ist über die Scan-Oberfläche von AVG über die Schaltfläche ***Scan-Ergebnisse*** verfügbar. Im Dialog wird eine Liste aller vorher gestarteten Scans und Informationen zu deren Ergebnissen angezeigt:

- ***Name*** – Scan-Ziel. Dabei kann es sich entweder um den Namen eines vordefinierten Scans oder um einen Namen handeln, den Sie Ihrem eigenen geplanten Scan gegeben haben. Jeder Name enthält ein Symbol, das das Scan-Ergebnis anzeigt:

  – Ein grünes Symbol zeigt an, dass beim Scan keine Infektion gefunden wurde

  – Ein blaues Symbol zeigt an, dass beim Scan eine Infektion gefunden, das infizierte Objekt jedoch automatisch entfernt wurde

  – Ein rotes Symbol zeigt an, dass beim Scan eine Infektion gefunden wurde, die nicht entfernt werden konnte!

  Jedes Symbol kann entweder ganz oder halb angezeigt werden. Ein vollständig angezeigtes Symbol zeigt an, dass ein Scan vollständig abgeschlossen und korrekt beendet wurde. Ein unvollständig angezeigtes Symbol zeigt an, dass der Scan unterbrochen oder abgebrochen wurde.

  Hinweis: *Genauere Informationen zu jedem Scan finden Sie im Dialog **Scan-Ergebnisse**, auf den Sie über die Schaltfläche **Details ansehen** (im unteren Teil des Dialogs) zugreifen können.*



- ***Startzeit*** – Datum und Uhrzeit des gestarteten Scans
- ***Endzeit*** – Datum und Uhrzeit des Scan-Endes
- ***Gescannte Objekte*** – Anzahl der gescannten Objekte
- ***Infektionen*** – Anzahl der erkannten/entfernten Vireninfektionen
- ***Spyware*** – Anzahl der erkannten/entfernten Spyware
- ***Warnungen*** – Anzahl der erkannten verdächtigen Objekte
- ***Rootkits*** – Anzahl der erkannten Rootkits
- ***Informationen zum Scan-Protokoll*** – Information zum Ablauf und zum Ergebnis des Scans (normalerweise nach dessen Abschluss oder bei Unterbrechung)

Schaltflächen

Im Dialog ***Übersicht über Scan-Ergebnisse*** stehen folgende Schaltflächen zur Verfügung:

- ***Details ansehen*** – Klicken Sie auf diese Schaltfläche, um in den Dialog ***Scan-Ergebnisse*** zu wechseln und genaue Daten zu einem ausgewählten Scan anzuzeigen
- ***Ergebnis löschen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Eintrag aus der Übersicht der Scan-Ergebnisse zu löschen
- ***Zurück*** – Mit dieser Schaltfläche gelangen Sie zurück zum Standarddialog der Scan-Oberfläche von AVG

10.7. Details zu den Scan-Ergebnissen

Wenn im Dialog ***Übersicht über Scan-Ergebnisse*** ein bestimmter Scan ausgewählt wurde, können Sie anschließend auf ***Details ansehen*** klicken und so zum Dialog ***Scan-Ergebnisse*** wechseln, in dem Sie genauere Informationen zum Ablauf und dem Ergebnis des ausgewählten Scans erhalten.

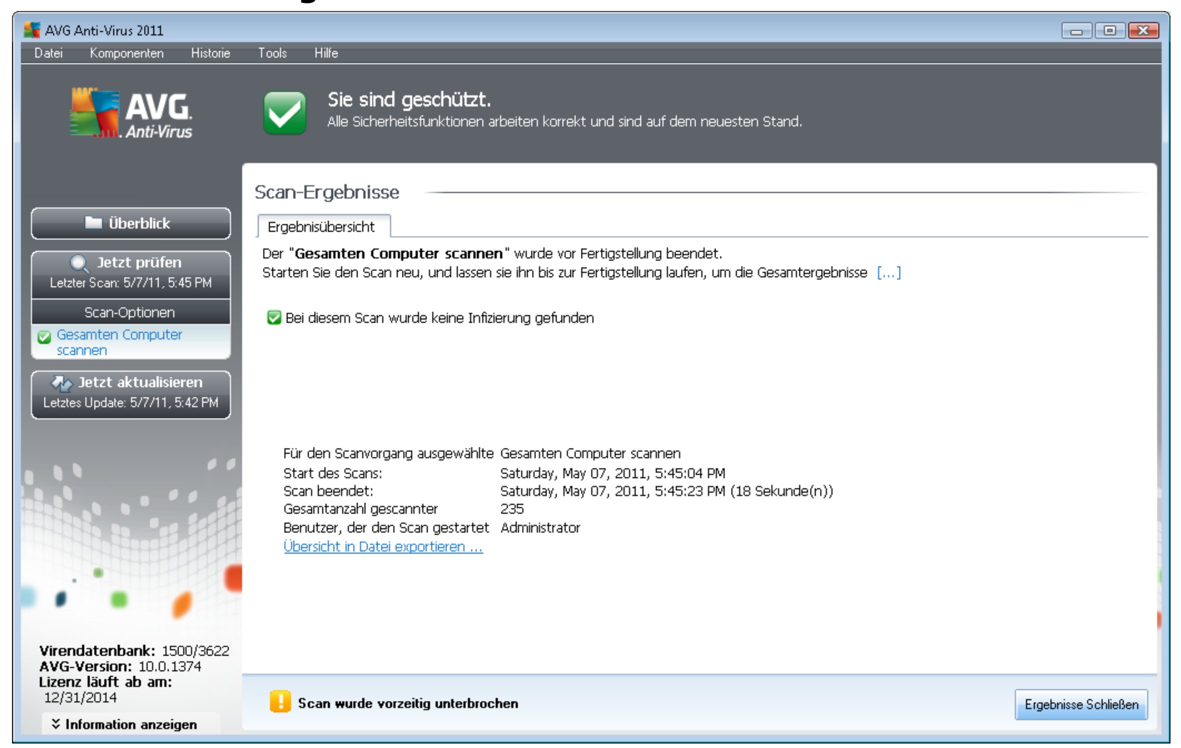
Dieser Dialog ist weiter in mehrere Reiter unterteilt:

- ***Ergebnisübersicht*** – Dieser Reiter wird immer angezeigt und enthält statistische Daten zum Scan-Verlauf
- ***Infektionen*** – Dieser Reiter wird nur angezeigt, wenn beim Scan eine Vireninfektion erkannt wurde
- ***Spyware*** – Dieser Reiter wird nur angezeigt, wenn beim Scan Spyware erkannt wurde
- ***Warnungen*** – Dieser Reiter wird angezeigt, wenn während eines Scans Cookies erkannt wurden
- ***Rootkits*** – Dieser Reiter wird nur angezeigt, wenn beim Scan Rootkits erkannt wurden



- ***Information*** – Dieser Reiter wird nur angezeigt, wenn potentielle Bedrohungen erkannt wurden und diese nicht in einer der oben genannten Kategorien eingeordnet werden konnten; der Reiter zeigt dann eine Warnbenachrichtigung zu diesem Fund an. Sie finden dort auch Informationen zu Objekten, die nicht gescannt werden können (z. B. kennwortgeschützte Archive).

10.7.1. Reiter „Ergebnisübersicht"



Auf dem Reiter ***Scan-Ergebnisse*** finden Sie eine genauere Statistik mit folgenden Informationen:

- Erkannte Vireninfektionen / Spyware
- Entfernte Vireninfektionen / Spyware
- Anzahl der Vireninfektionen / Spyware, die nicht entfernt oder geheilt werden konnte

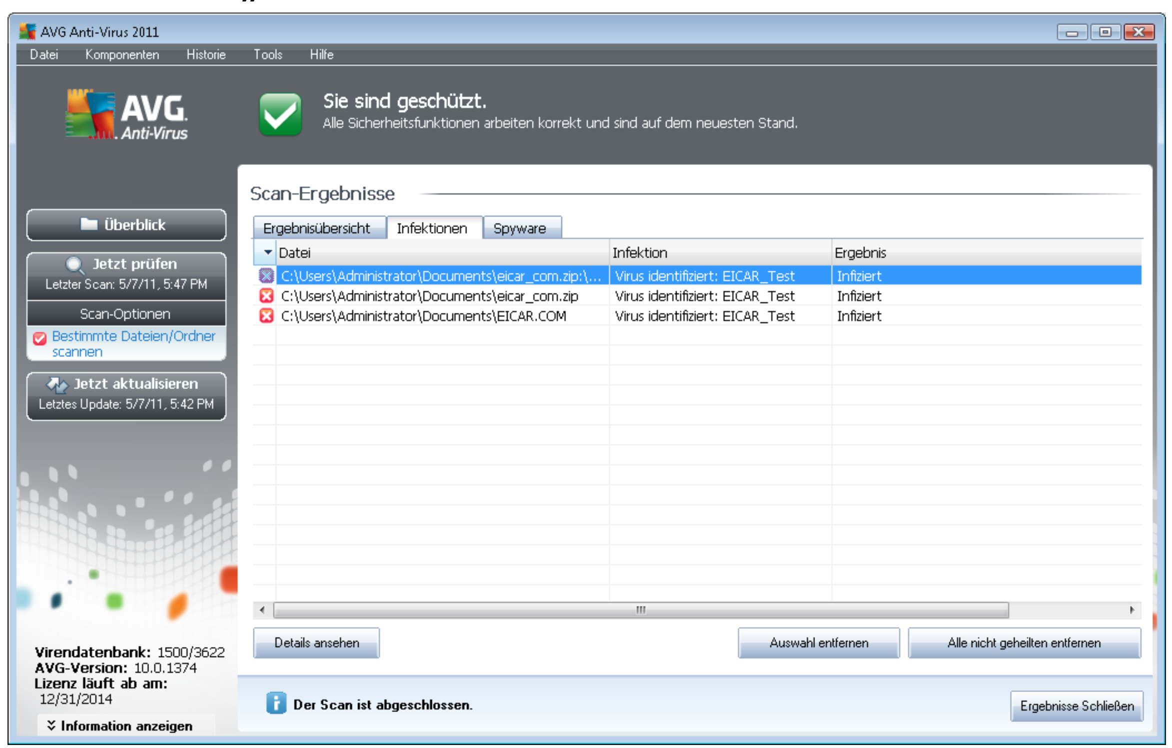
Darüber hinaus erhalten Sie Informationen zu Datum und Uhrzeit des gestarteten Scans, zur Gesamtanzahl der gescannten Objekte, zur Scan-Dauer sowie zur Anzahl der Fehler, die beim Scan auftraten.

Schaltflächen

In diesem Dialog steht lediglich eine Schaltfläche zur Verfügung. Mit der Schaltfläche ***Ergebnisse schließen*** kehren Sie zum Dialog ***Übersicht über Scan-Ergebnisse*** zurück.



10.7.2. Reiter „Infektionen"



Der Reiter ***Infektionen*** wird nur dann im Dialog ***Scan-Ergebnisse*** angezeigt, wenn während des Scans eine Vireninfektion erkannt wurde. Dieser Reiter ist in drei Bereiche unterteilt, die folgende Informationen enthalten:

- ***Datei*** – Der vollständige Pfad zum ursprünglichen Standort des infizierten Objekts
- ***Infektion*** – Name des erkanntenVirus (*genauere Informationen zu bestimmten Viren finden Sie online in der Virenenzyklopädie*)
- ***Ergebnis*** – Hier wird der aktuelle Status des beim Scan erkannten Objekts definiert:
    - o ***Infiziert*** – Das infizierte Objekt wurde erkannt und an seinem ursprünglichen Ort belassen (beispielsweise, wenn Sie die *Option für automatisches Heilen in bestimmten Scan-Einstellungen deaktiviert haben)*
    - o ***Geheilt*** – Das infizierte Objekt wurde automatisch geheilt und an seinem ursprünglichen Ort belassen
    - o ***In Virenquarantäne verschoben*** – Das infizierte Objekt wurde in die ***Virenquarantäne*** verschoben
    - o ***Gelöscht*** – Das infizierte Objekt wurde gelöscht
    - o ***Zu PUP-Ausnahmen hinzugefügt*** – Der Fund wurde als Ausnahme eingestuft und zur Liste der PUP-Ausnahmen hinzugefügt (*konfiguriert im Dialog* ***PUP-Ausnahmen***



in den erweiterten Einstellungen)

- ***Gesperrte Datei – nicht getestet*** – Das betreffende Objekt ist gesperrt und kann daher nicht von AVG gescannt werden

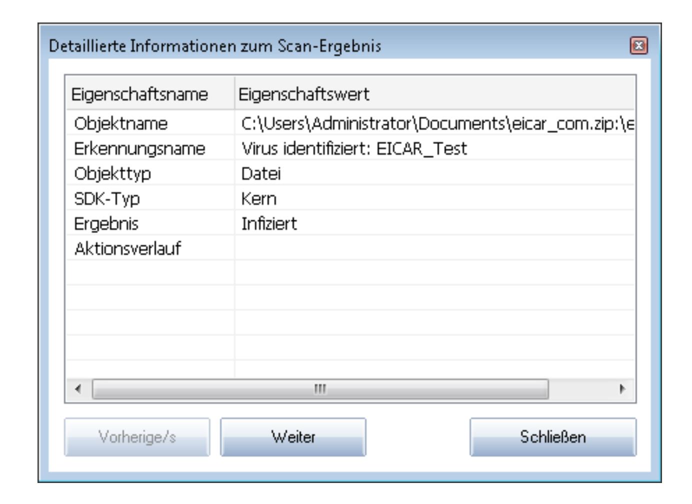
- ***Potentiell gefährliches Objekt*** – Das Objekt wurde als potentiell gefährlich, aber nicht als infiziert erkannt (*es könnte zum Beispiel Makros enthalten*); diese Information dient lediglich als Warnung

- ***Neustart erforderlich, um die Aktion abzuschließen*** – Das infizierte Objekt kann nicht entfernt werden. Um es vollständig zu entfernen, müssen Sie Ihren Computer neu starten

Schaltflächen

In diesem Dialog stehen drei Schaltflächen zur Verfügung:

- ***Details ansehen*** – Diese Schaltfläche öffnet einen neuen Dialog ***Detaillierte Objektinformationen***:



In diesem Dialog finden Sie weitere Informationen zum erkannten, infizierten Objekt (*z. B. Name und Speicherort des infizierten Objekts, Objekttyp, SDK-Typ, Erkennungsergebnis und Aktionsverlauf des infizierten Objekts*). Mit den Schaltflächen ***Vorherige/s*** bzw. ***Weiter*** können Sie Informationen zu bestimmten Funden anzeigen. Klicken Sie auf die Schaltfläche ***Schließen***, um den Dialog zu verlassen.

- ***Auswahl entfernen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Fund in die ***Virenquarantäne*** zu verschieben

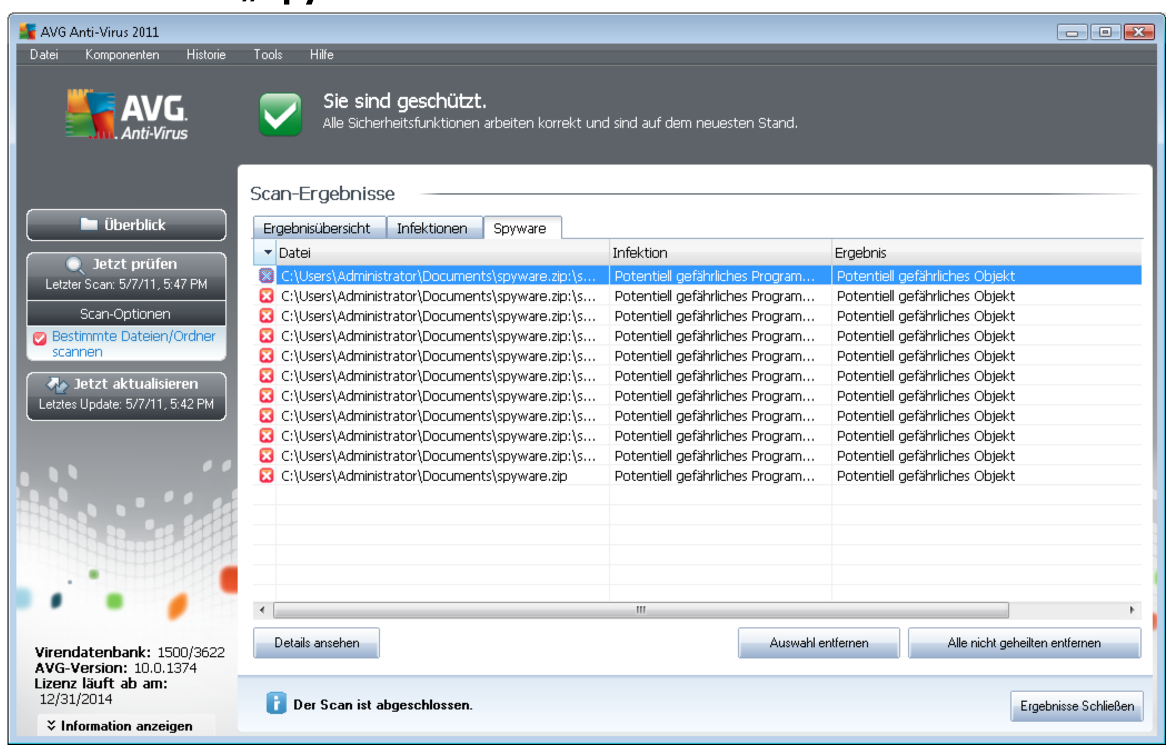
- ***Alle nicht geheilten entfernen*** – Diese Schaltfläche löscht alle Funde, die nicht geheilt oder in die ***Virenquarantäne*** verschoben werden können

- ***Zurück*** – Die detaillierte Informationsübersicht wird geschlossen, und Sie gelangen zurück



zum Dialog [***Übersicht über Scan-Ergebnisse***]

10.7.3. Reiter „Spyware“



Der Reiter ***Spyware*** wird nur dann im Dialog ***Scan-Ergebnisse*** angezeigt, wenn beim Scan [Spyware] erkannt wurde. Dieser Reiter ist in drei Bereiche unterteilt, die folgende Informationen enthalten:

- ***Datei*** – Der vollständige Pfad zum ursprünglichen Standort des infizierten Objekts
- ***Infektionen*** – Name der erkannten[Spyware] (*genauere Informationen zu bestimmten Viren finden Sie in der* [***Virenenzyklopädie***] *online*)
- ***Ergebnis*** – Hier wird der aktuelle Status des beim Scan erkannten Objekts definiert:
  - o ***Infiziert*** – Das infizierte Objekt wurde erkannt und an seinem ursprünglichen Ort belassen (beispielsweise, wenn Sie die [Option für automatisches Heilen] in bestimmten Scan-Einstellungen deaktiviert haben)
  - o ***Geheilt*** – Das infizierte Objekt wurde automatisch geheilt und an seinem ursprünglichen Ort belassen
  - o ***In Virenquarantäne verschoben*** – Das infizierte Objekt wurde in die [***Virenquarantäne***] ***verschoben***
  - o ***Gelöscht*** – Das infizierte Objekt wurde gelöscht
  - o ***Zu PUP-Ausnahmen hinzugefügt*** – Der Fund wurde als Ausnahme eingestuft und



zur Liste der PUP-Ausnahmen hinzugefügt (*konfiguriert im Dialog* ***PUP-Ausnahmen*** *in den erweiterten Einstellungen*)

- o ***Gesperrte Datei – nicht getestet*** – Das betreffende Objekt ist gesperrt und kann daher nicht von AVG gescannt werden

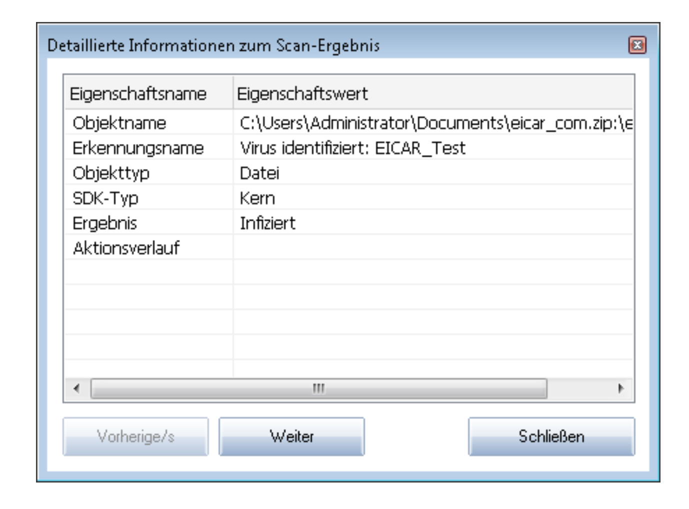
- o ***Potentiell gefährliches Objekt*** – Das Objekt wurde als potentiell gefährliches Objekt, aber nicht als infiziert erkannt (es enthält zum Beispiel möglicherweise Makros); diese Information dient lediglich als Warnung

- o ***Neustart erforderlich, um die Aktion abzuschließen*** – Das infizierte Objekt kann nicht entfernt werden. Um es vollständig zu entfernen, müssen Sie Ihren Computer neu starten

Schaltflächen

In diesem Dialog stehen drei Schaltflächen zur Verfügung:

- ***Details ansehen*** – Diese Schaltfläche öffnet einen neuen Dialog ***Detaillierte Objektinformationen***:



In diesem Dialog finden Sie weitere Informationen zum erkannten, infizierten Objekt (*z. B. Name und Speicherort des infizierten Objekts, Objekttyp, SDK-Typ, Erkennungsergebnis und Aktionsverlauf des infizierten Objekts*). Mit den Schaltflächen ***Vorherige/s*** bzw. ***Weiter*** können Sie Informationen zu bestimmten Funden anzeigen. Klicken Sie auf die Schaltfläche ***Schließen***, um den Dialog zu verlassen.

- ***Auswahl entfernen*** – Klicken Sie auf diese Schaltfläche, um den ausgewählten Fund in die ***Virenquarantäne*** zu verschieben

- ***Alle nicht geheilten entfernen*** – Diese Schaltfläche löscht alle Funde, die nicht geheilt oder in die ***Virenquarantäne***



- ***Zurück*** – Die detaillierte Informationsübersicht wird geschlossen, und Sie gelangen zurück zum Dialog ***Übersicht über Scan-Ergebnisse***

10.7.4. Reiter „Warnungen"

Auf dem Reiter ***Warnungen*** werden Informationen zu „verdächtigen" Objekten (*normalerweise Dateien*) angezeigt, die beim Scan erkannt wurden. Wenn diese Dateien von ***Residenter Schutz*** erkannt werden, wird der Zugriff auf diese Dateien blockiert. Typische Funde dieser Art sind beispielsweise folgende: Versteckte Dateien, Cookies, verdächtige Registrierungsschlüssel, kennwortgeschützte Dokumente oder Archive usw. Diese Dateien stellen keine direkte Bedrohung für Ihren Computer oder Sicherheit dar. Informationen zu diesen Dateien können bei der Erkennung von Adware oder Spyware auf Ihrem Computer nützlich sein. Wenn diese Warnungen nur nach einem AVG-Scan ausgegeben werden, ist keine Aktion nötig.

Dies ist eine kurze Beschreibung der bekanntesten Beispiele solcher Objekte:

- ***Versteckte Dateien*** – Versteckte Dateien sind in Windows standardmäßig nicht sichtbar, und bestimmte Viren oder andere Bedrohungen können versuchen, der Erkennung durch das Speichern ihrer Dateien mit diesem Attribut zu umgehen. Wenn Ihr AVG eine versteckte Datei meldet, die verseucht sein könnte, können Sie diese in die ***AVG Virenquarantäne*** verschieben.

- ***Cookies*** – Cookies sind reine Textdateien, die von Webseiten dazu verwendet werden, benutzerbezogene Informationen zu speichern. Diese Informationen werden später verwendet, um benutzerdefinierte Layouts von Websites zu laden, Benutzernamen einzutragen usw.

- ***Verdächtige Registrierungsschlüssel*** – Manche Malware speichert Informationen in der Windows-Registrierung, um sicherzustellen, dass sie beim Hochfahren geladen wird oder um ihre Auswirkung auf das Betriebssystem zu erweitern.

10.7.5. Reiter „Rootkits"

Auf dem Reiter ***Rootkits*** werden Informationen zu Rootkits angezeigt, die beim ***Anti-Rootkit-Scan*** erkannt wurden.

Ein ***Rootkit*** ist ein Programm, das ohne Genehmigung der Systembesitzer oder berechtigten Manager die Kontrolle über ein Computersystem übernimmt. Ein Zugriff auf die Hardware ist meist nicht erforderlich, da ein Rootkit darauf abzielt, die Kontrolle über das Betriebssystem, das auf der Hardware ausgeführt wird, zu übernehmen. Rootkits verbergen ihre Existenz auf dem System üblicherweise, indem sie die standardmäßigen Sicherheitsmechanismen des Betriebssystems außer Kraft setzen oder umgehen. Oft handelt es sich bei diesen Programmen gleichzeitig um Trojaner, die bei Benutzern den Eindruck erwecken, sie könnten ohne Risiko auf ihren Systemen ausgeführt werden. Dies wird mit Techniken wie dem Verbergen von ausgeführten Prozessen vor Überwachungsprogrammen oder dem Verbergen von Dateien oder Systemdaten vor dem Betriebssystem erzielt.

Dieser Reiter ist ähnlich aufgebaut wie der Reiter ***Infektionen*** oder ***Spyware***.



10.7.6. Reiter „Informationen"

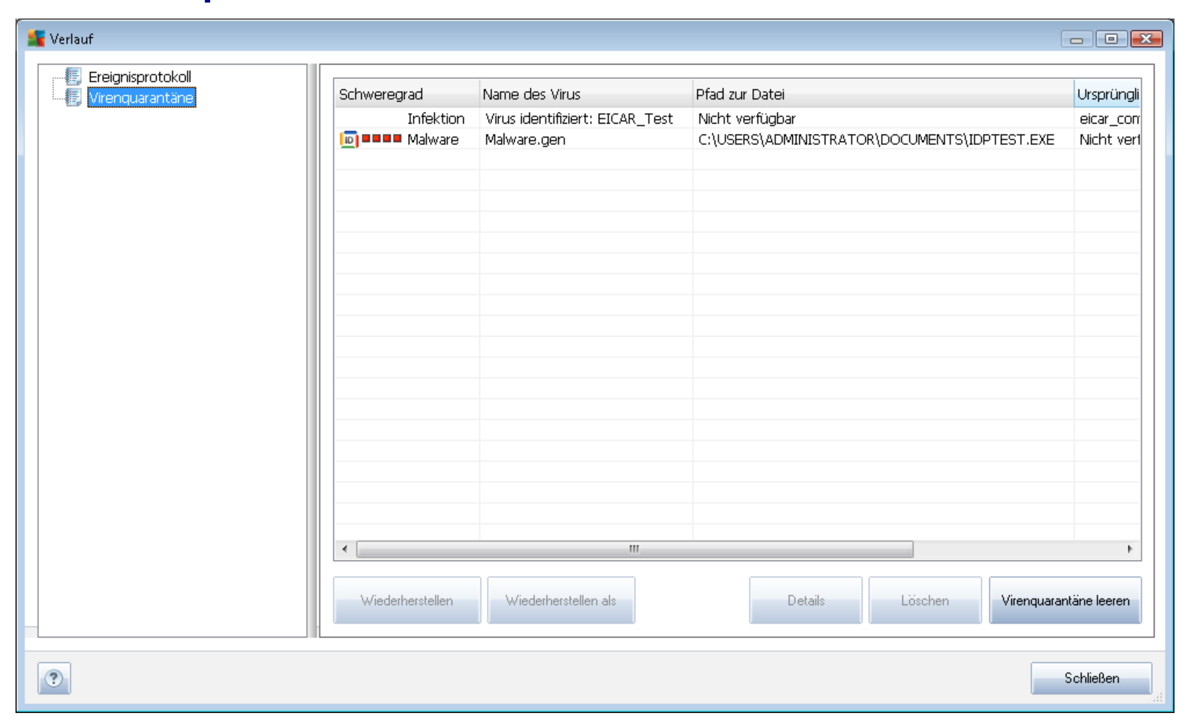
Der Reiter ***Informationen*** enthält Daten über „Funde", die nicht als Infektionen, Spyware usw. eingestuft werden können. Sie können nicht eindeutig als gefährlich klassifiziert werden, müssen jedoch trotzdem beachtet werden. AVG-Scan kann Dateien erkennen, die möglicherweise nicht infiziert, aber verdächtig sind. Diese Dateien werden entweder als ***Warnung*** oder als ***Information*** gemeldet.

Die ***Information*** zum Schweregrad kann aus einem der folgenden Gründe angezeigt werden:

- ***Run-time packed*** – Die Datei wurde mit einem unüblichen Run-Time-Packer gepackt, was auf einen Versuch hinweisen kann, den Scan der Datei zu verhindern. Nicht jeder Bericht über eine solche Datei weist jedoch auf ein Virus hin.
- ***Run-time packed recursive*** – Ähnlich wie oben, jedoch weniger häufig unter gebräuchlicher Software. Solche Dateien sind verdächtig und sollten entfernt oder zur Analyse eingesendet werden.
- ***Kennwortgeschützte Dokumente oder Archive*** – Kennwortgeschützte Dateien können von AVG (*bzw. anderen Anti-Malware-Programmen*) nicht gescannt werden.
- ***Dokument mit Makros*** – Das gemeldete Dokument enthält Makros, die möglicherweise schädlich sind.
- ***Versteckte Erweiterung*** – Dateien mit versteckten Erweiterungen können beispielsweise wie Bilder aussehen, sind jedoch in Wahrheit ausführbare Dateien (*z. B. bild.jpg.exe*). Die zweite Erweiterung ist standardmäßig in Windows nicht sichtbar. AVG berichtet solche Dateien, um ein versehentliches Öffnen dieser Dateien zu verhindern.
- ***Falscher Dateipfad*** – Wenn eine wichtige Systemdatei nicht vom Standardpfad ausgeführt wird (*winlogon.exe wird z. B. nicht aus dem Windows-Ordner ausgeführt*), meldet AVG diese Unstimmigkeit. In einigen Fällen verwenden Viren die Namen von Standardsystemprozessen, damit ihr Vorhandensein im System weniger auffällt.
- ***Gesperrte Datei*** – Die gemeldete Datei ist gesperrt und kann von AVG nicht gescannt werden. Das bedeutet üblicherweise, dass diese Datei dauerhaft vom System verwendet wird (*z. B. Auslagerungsdateien*).



10.8. Virenquarantäne



Virenquarantäne ist eine sichere Umgebung zur Verwaltung von verdächtigen und infizierten Objekten, die von AVG beim Scan erkannt wurden. Sobald beim Scan ein infiziertes Objekt erkannt wird und AVG dieses nicht automatisch heilen kann, werden Sie gefragt, wie dieses verdächtige Objekt behandelt werden soll. Es wird empfohlen, das Objekt zur weiteren Behandlung in die ***Virenquarantäne*** zu verschieben. Die ***Virenquarantäne*** ist in erster Linie dazu da, entfernte Dateien so lange zu speichern, bis sie an ihrem ursprünglichen Speicherort nicht mehr benötigt werden. Wenn das Fehlen der Datei Probleme bereitet, können Sie die fragliche Datei zur Analyse senden oder sie an ihrem ursprünglichen Speicherort wiederherstellen.

Die Oberfläche der ***Virenquarantäne*** wird in einem eigenen Fenster geöffnet, in dem eine Informationsübersicht über infizierte Objekte angezeigt wird, die sich in der Quarantäne befinden:

- ***Schweregrad*** – Wenn Sie sich zur Installation der Komponente ***Identitätsschutz*** in **AVG Anti-Virus 2011** entschieden haben, wird eine grafische Identifizierung des entsprechenden Schweregrads des Prozesses auf einer vierstufigen Skala von unbedenklich (■□□□) bis sehr gefährlich (■■■■) angezeigt sowie die Informationen zur Infektionsart (*basierend auf ihrer Infektionsstufe – alle aufgelisteten Objekte können tatsächlich oder potentiell infiziert sein*)

- ***Name des Virus*** – Der Name der erkannten Infektion wird entsprechend der ***Virenenzyklopädie*** (online) angegeben

- ***Pfad zur Datei*** – Der vollständige Pfad zum ursprünglichen Standort der infizierten Datei

- ***Ursprünglicher Objektname*** – Alle hier aufgelisteten Objekte wurden von AVG während des Scanvorgangs mit dem Standardnamen gekennzeichnet. Wenn das Objekt einen



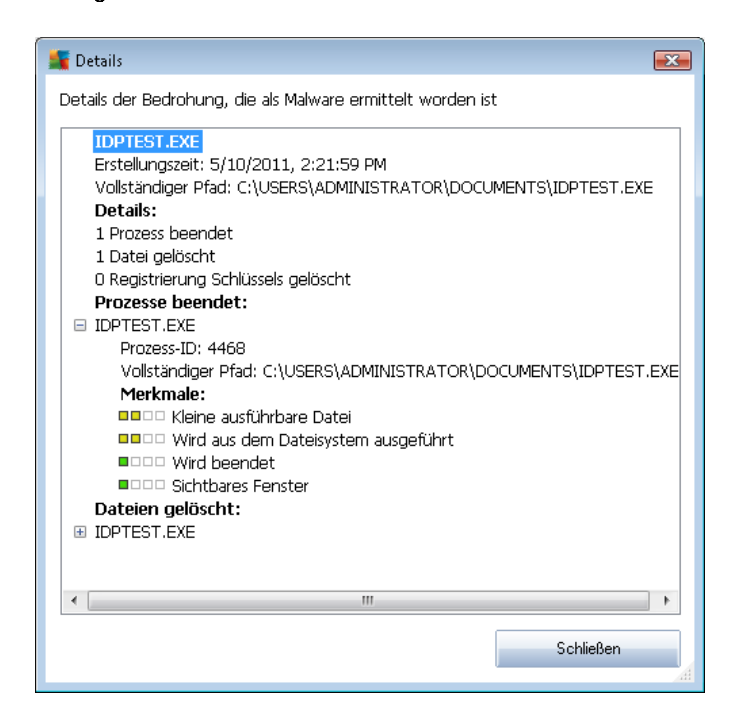
bekannten ursprünglichen Namen hat (*z. B. der Name eines eMail-Anhangs, der nicht mit dem eigentlichen Inhalt des Anhangs übereinstimmt*), wird der Name in dieser Spalte angegeben.

- ***Speicherdatum*** – Datum und Uhrzeit, zu dem die verdächtige Datei erkannt und in die ***Virenquarantäne verschoben wurde***

Schaltflächen

Auf der Oberfläche der ***Virenquarantäne*** stehen folgende Schaltflächen zur Verfügung:

- ***Wiederherstellen*** – Die infizierte Datei wird zurück zu ihrem ursprünglichen Standort auf Ihrer Festplatte verschoben
- ***Wiederherstellen als*** – Die infizierte Datei wird in den ausgewählten Ordner verschoben
- ***Details*** – Diese Schaltfläche gilt nur für Bedrohungen, die von ***Identitätsschutz*** gefunden wurden. Nach dem Anklicken wird eine zusammenfassende Übersicht über die Bedrohungsdetails angezeigt (*welche Dateien/Prozesse sind betroffen, Merkmale des Prozesses usw.*). Bitte beachten Sie, dass die Schaltfläche bei allen anderen Bedrohungen, die nicht von Identitätsschutz entdeckt wurden, ausgegraut und inaktiv ist!



- ***Löschen*** – Die infizierte Datei wird vollständig und unwiederbringlich aus der ***Virenquarantäne*** gelöscht
- ***Virenquarantäne leeren*** - Alle Objekte werden vollständig aus der ***Virenquarantäne*** entfernt. Durch das Entfernen der Dateien aus der ***Virenquarantäne*** werden diese Dateien unwiderruflich von der Festplatte entfernt (*sie werden nicht in den Papierkorb verschoben*).



11. AVG Updates

Die regelmäßige Aktualisierung von AVG ist entscheidend, damit alle neu entdeckten Viren so früh wie möglich erkannt werden.

Da AVG-Updates nicht nach einem festen Zeitplan, sondern entsprechend der Anzahl und des Schweregrads neuer Bedrohungen zur Verfügung gestellt werden, wird empfohlen, mindestens einmal täglich (oder bei Bedarf sogar öfter) eine Prüfung auf neue Updates durchzuführen. Dadurch können Sie sicherstellen, dass Ihr **AVG Anti-Virus 2011** auch tagsüber auf dem aktuellsten Stand ist.

11.1. Updatestufen

Sie können in AVG eine von zwei Updatestufen auswählen:

- ***Definitionsupdates*** umfassen Änderungen, die für zuverlässigen Viren-Schutz erforderlich sind. In der Regel umfasst sie keine Änderungen am Code und es wird nur die Virendatenbank aktualisiert. Dieses Update sollte durchgeführt werden, sobald es verfügbar ist.

- ***Das Programmupdate*** enthält verschiedene Programmänderungen, -ausbesserungen und -verbesserungen.

Beim Planen von Updates können Sie auswählen, welche Prioritätsstufe heruntergeladen und angewendet werden soll.

Hinweis: *Wenn sich ein geplantes Programm-Update und ein geplanter Scan zeitlich überschneiden, wird der Scan unterbrochen, da das Update eine höhere Priorität hat.*

11.2. Updatetypen

Sie können zwischen zwei Aktualisierungstypen wählen:

- ***Eine Aktualisierung On-Demand*** ist ein sofortiges Update von AVG, das bei Bedarf jederzeit durchgeführt werden kann.

- ***Geplante Aktualisierung*** – Innerhalb von AVG können Sie auch einen Aktualisierungsplan voreinstellen. Die geplante Aktualisierung wird dann regelmäßig zu den festgelegten Zeiten ausgeführt. Immer wenn neue Aktualisierungsdateien an dem angegebenen Speicherort verfügbar sind, werden sie entweder direkt über das Internet oder das Netzwerkverzeichnis heruntergeladen. Wenn keine neuen Aktualisierungen verfügbar sind, passiert nichts.

11.3. Updatevorgang

Der Updateprozess kann bei Bedarf unmittelbar gestartet werden, indem Sie auf den Quick Link ***Jetzt aktualisieren*** klicken. Dieser Link steht Ihnen jederzeit in allen Dialogen der Benutzeroberfläche von AVG zur Verfügung. Es empfiehlt sich jedoch, Updates regelmäßig entsprechend dem Updatezeitplan durchzuführen, der in der Komponente Updatemanager bearbeitet werden kann.

Wenn Sie das Update starten, überprüft AVG zunächst, ob neue Updatedateien zur Verfügung

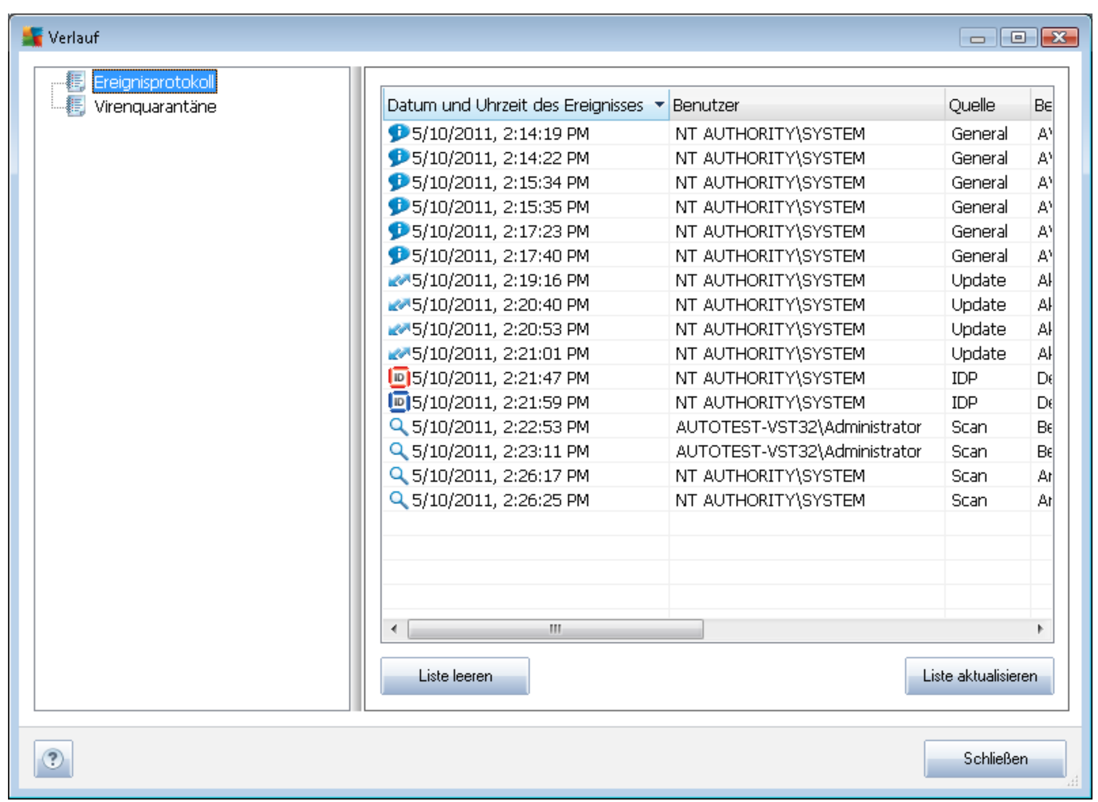


stehen. Wenn dies der Fall ist, lädt AVG diese eigenständig herunter und startet den Updateprozess. Während des Updateprozesses werden Sie zur Benutzeroberfläche ***Update*** weitergeleitet, wo der Fortschritt des Updates grafisch dargestellt und wie eine Übersicht über die statistischen Parameter (*Größe der Updatedatei, empfangene Daten, Download-Geschwindigkeit, verstrichene Zeit usw.*) angezeigt wird.

Hinweis*: Vor einem Update des AVG-Programms wird ein Systemwiederherstellungspunkt erstellt. Wenn der Updatevorgang fehlschlägt und Ihr Betriebssystem abstürzt, können Sie ab diesem Punkt Ihr Betriebssystem in der ursprünglichen Konfiguration wiederherstellen. Diese Option kann über Start/Programme/Zubehör/Systemprogramme/Systemwiederherstellung aufgerufen werden. Änderungen sollten jedoch nur von erfahrenen Benutzern vorgenommen werden!*



12. Ereignisprotokoll



Der Dialog ***Historie*** kann im Systemmenü über die Optionen ***Historie/Ereignisprotokoll*** geöffnet werden. In diesem Dialog finden Sie eine Zusammenfassung aller wichtigen Ereignisse, die während der Ausführung von **AVG Anti-Virus 2011** aufgetreten sind. In der ***Historie*** werden folgende Ereignistypen aufgezeichnet:

- Informationen über Updates der AVG-Anwendung
- Start, Ende oder Unterbrechung des Scans (*einschließlich automatisch ausgeführter Tests*)
- Ereignisse in Verbindung mit der Virenerkennung (*durch Residenten Schutz oder einen Scan*), einschließlich des Ortes, an dem das Ereignis aufgetreten ist
- Andere wichtige Ereignisse

Für jedes Ereignis werden die folgenden Informationen aufgelistet:

- ***Datum und Uhrzeit des Ereignisses*** gibt das exakte Datum und die exakte Uhrzeit des Ereignisses an.
- ***Benutzer*** gibt an, von wem das Ereignis initialisiert wurde.
- ***Quelle*** gibt die Quellkomponente oder den Teil des AVG-Systems an, von der bzw. dem



das Ereignis ausgelöst wurde

- ***Beschreibung des Ereignisses*** gibt eine kurze Zusammenfassung der tatsächlichen Geschehnisse.

Schaltflächen

- ***Liste leeren*** – Alle Einträge der Ereignisliste werden gelöscht
- ***Liste aktualisieren*** – Alle Einträge der Ereignisliste werden aktualisiert



13. FAQ und technischer Support

Bei Problemen mit AVG, egal ob diese geschäftlicher oder technischer Art sind, konsultieren Sie bitte den Abschnitt ***FAQ*** auf der Website von AVG (http://www.avg.com/de/).

Falls Sie auf diese Weise keine Lösung für Ihr Problem finden, wenden Sie sich bitte per eMail an den technischen Support. Verwenden Sie bitte das Kontaktformular, das im Systemmenü unter ***Hilfe / Onlinehilfe*** zur Verfügung steht.